

Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации
Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

**Международная научно-практическая конференция
(17 апреля 2025 г.)**

Сборник научных трудов

1 электронный оптический диск (CD-R)
Текстовое электронное издание

Научное электронное издание

Москва
Московский университет
МВД России имени В.Я. Кикотя

2025

© Московский университет
МВД России имени В.Я. Кикотя, 2025
ISBN 978-5-9694-1638-3

УДК 343.2/.7
ББК 67.51
П83

Рецензенты:

заместитель начальника УВД по ЗАО ГУ МВД России по г. Москве
К. Ю. Лернер; заместитель начальника УВД по ЗАО ГУ МВД России
по г. Москве – начальник СУ **Д. В. Зобнин**; старший участковый
уполномоченный полиции УМВД России по городскому округу Химки
А. И. Герасин

Составитель *А. В. Константинов*, заместитель начальника кафедры
противодействия преступлениям в сфере информационно-телекоммуникационных
технологий Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

**П83 Противодействие преступлениям в сфере информационно-телекомму-
никационных технологий** : Международная научно-практическая конфе-
ренция, 17 апреля 2025 г. : сборник научных трудов / [сост. А. В. Константи-
нов]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2025. –
631 с. – 1 электронный оптический диск (CD-R). – Системные требования :
CPU 1,5 ГГц ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места
на жестком диске.
ISBN 978-5-9694-1638-3

Сборник научных трудов «Противодействие преступлениям в сфере информационно-телекоммуникационных технологий» посвящен теоретическим, правовым, методическим и организационным проблемам противодействия преступлениям в указанной сфере.

Материалы сборника могут быть полезны для курсантов и слушателей образовательных организаций МВД России, преподавателей, адъюнктов и аспирантов, а также для практических работников органов внутренних дел и всех интересующихся данной тематикой.

Научное электронное издание

Минимальные системные требования: CPU 1,5 ГГц; RAM 512 Мб;
Windows XP SP3; 1 Гб свободного места на жестком диске

© Московский университет
МВД России имени В.Я. Кикотя, 2025

Издание подготовлено
с помощью программного обеспечения Microsoft Word

В авторской редакции
Компьютерная верстка: *Горбунова Т. С., Жукова О. И.*

Подписано к изданию 20.08.2025
Объем издания: 5,33 МБ
Тираж: 6 электронных оптических дисков (CD-R)

ISBN 978-5-9694-1638-3



Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
<https://мосу.мвд.рф>, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

РАЗДЕЛ I. Трибуна руководителя

Пушкарев В. В.

Ущерб информационной инфраструктуре: глобальный анализ норм и правоприменительной практики.....13

Зайцев О. А.

Особенности доказывания в ходе производства по уголовному делу в условиях цифровой трансформации.....18

Тисен О. Н.

Особенности доказывания преступлений, совершенных с использованием криптовалют: следственная и судебная практика 23

Минаков С. С.

О развитии информационных систем по противодействию преступности 38

Ярмак К. В.

Реализация статуса базовой организации государств – участников СНГ с использованием цифрового сопровождения образовательного процесса 42

Константинов А. В.

OSINT как объект уголовно-правового исследования.....47

Эрдниева А. С.

Об особенностях подготовки иностранных специалистов по информационной безопасности на современном этапе 50

Михайленко Н. В.

Ключи от разума: социальная инженерия как объект правового регулирования.....56

Власов П. Е.

Некоторые из допустимых направлений использования искусственных когнитивных систем в уголовном судопроизводстве 62

Лахтиков Д. Н.

Нейтрализация финансовой составляющей как элемент противодействия киберпреступности 67

РАЗДЕЛ II. Использование цифровых технологий в целях противодействия преступлениям в сфере информационно-телекоммуникационных технологий

Анаев И. Х., Солодар Д. Д.

Использование искусственного интеллекта в деятельности оперативных подразделений органов внутренних дел.....72

Баранов А. А., Соломатина Е. А.

К вопросу о мерах противодействия преступлениям, совершаемым против несовершеннолетних с применением информационно-телекоммуникационных технологий 78

<i>Григорьев Д. А., Лаптев Д. Д.</i> Современные механизмы легализации преступных доходов с использованием информационно-телекоммуникационных технологий: вызовы для правоохранительной системы и проблемы противодействия	82
<i>Ерлан Б. Т.</i> Тенденции развития кибербезопасности и информационной безопасности в предупреждении современных угроз	92
<i>Калашников И. В., Скворцова К. Р.</i> Основные направления предупреждения и противодействия киберпреступлениям в Российской Федерации	96
<i>Колбасина Е. Е., Василенко Д. И.</i> Использование блокчейн-технологии в преступной деятельности: механизмы, угрозы и методы противодействия	101
<i>Корнева Ю. Ю.</i> Психология несовершеннолетних в условиях цифровой среды: риски вовлечения в ИТТ-преступления и виктимизация	105
<i>Кубасов И. А.</i> Анализ международного опыта противодействия киберпреступлениям	109
<i>Лакомская М. Ю.</i> Использование искусственного интеллекта в расследовании преступлений: возможности и недостатки	114
<i>Мамий А. Х.</i> Идентификация и устранение предвзятости в профилировании подозреваемых в киберпреступлениях.....	117
<i>Поликарова Е. В.</i> Анализ современных методов мошенничества в сети Интернет: тенденции и прогнозы.....	121
<i>Попенков А. В.</i> Противодействие незаконной коллекторской деятельности в современном цифровом пространстве	127
<i>Пучков Г. Ю.</i> Анализ возможных направлений дальнейшего развития криминальных технологий с использованием искусственного интеллекта	130
<i>Рудин А. В.</i> Характеристика преступлений, совершенных с использованием искусственного интеллекта	136
<i>Савотченко С. Е., Симонцев Д. А., Акапьев В. Л.</i> Теоретические и практические аспекты правового регулирования использования искусственного интеллекта	140
<i>Савченко Е. А.</i> Правовые аспекты социального неравенства, связанные с «разноуровневым» доступом к возможностям искусственного интеллекта	145

<i>Смушкин А. Б.</i>	
Перспективы развития цифровых платформ правоохранительных органов	152
<i>Соломатина А. Г.</i>	
Инструменты и технологии для расследования преступлений, связанных с криптовалютами: анализ современных подходов и перспектив развития	157
<i>Терентьев А. А.</i>	
Применение имитационного моделирование в информационной безопасности сети связи специального назначения.....	161
<i>Токолов А. В.</i>	
Меры предупредительного характера, применяемые органами правопорядка, в целях обеспечения кибербезопасности в социальных сетях	164
<i>Трофимов В. Е.</i>	
Предупреждение мошеннических действий, совершаемых в сфере оборота цифровой валюты.....	170
<i>Фокин А. Д.</i>	
Телефонное мошенничество: уголовно-правовые и криминалистические аспекты противодействия.....	175
<i>Цурлуй О. Ю.</i>	
Роль криминалистической профилактики преступлений, совершаемых с использованием информационных технологий	180
<i>Чехович А. А.</i>	
Личность преступника, как элемент оперативно-розыскной характеристики несанкционированного доступа к компьютерной информации	185
<i>Шаевич А. А.</i>	
Организационно-правовые и этические проблемы использования нейросетей при расследовании преступлений	188
<i>Шайдаев М. Ш.</i>	
Противодействие преступлениям против половой неприкосновенности, половой свободы и нравственности, совершаемым с использованием информационно-коммуникационных технологий	192
<i>Шавловский А. Б.</i>	
Практические аспекты информационно-аналитических исследований открытых источников сети Интернет	198

РАЗДЕЛ III. Виды преступлений, связанных с распространением информации в информационно-телекоммуникационной сети Интернет

<i>Аксенов А. В.</i>	
Метод социальной инженерии, как средство достижения целей киберпреступлений	201
<i>Алексеева Г. П.</i>	
Хакерство как вид совершения киберпреступления XXI в.....	204

<i>Амбросенкова Д. С.</i> Проблемные вопросы и перспективы совершенствования законодательства Российской Федерации в области вебкам-индустрии	209
<i>Антюшина А. С.</i> Применение искусственного интеллекта (нейронных сетей) в деятельности полиции	213
<i>Байкова А. П.</i> Противодействие дистанционным хищениям: проблемные вопросы и пути решения	217
<i>Баканов Н. А.</i> Использование помощи населения при расследовании преступлений, совершенных с помощью информационных-телекоммуникационных технологий	222
<i>Белякова А. А.</i> Риски реальной личности под воздействием цифровизации и цифровой личности	228
<i>Бойко И. В.</i> Оперативно-разыскное противодействие мошенничествам, совершаемым с использованием криптовалют	231
<i>Брюзгин А. И.</i> Защита интернета вещей (IoT) от кибератак	235
<i>Булатова В. Д.</i> Правовое значение сотрудничества органов внутренних дел со СМИ в предупреждении преступлений в сфере информационно- телекоммуникационных технологий	239
<i>Буракова А. А.</i> Информационные технологии используемые в целях противодействия преступлениям	243
<i>Варванская А. В., Красовская М. А.</i> Особенности доказывания по делам, связанным с использованием блокчейна: сравнительно-правовой анализ	246
<i>Любовь М. В.</i> Типология и виды компьютерных атак на кредитные организации	261
<i>Вершинина И. О.</i> Кибербуллинг и его законодательное закрепление	268
<i>Веселова Д. А.</i> Безопасность в цифровом мире: от наивности к осознанной защите	272
<i>Власова Я. Э.</i> Уровень цифровизации в обществе и развитие в нем киберпреступности	276
<i>Волкова Ю. А.</i> Понятие и принципы функционирования Darknet	279

<i>Воронкова М. В., Нуреев Д. О.</i> Правовое регулирование криптовалюты в Европейском союзе	283
<i>Гавирова Г. А.</i> Методы борьбы с киберпреступностью	291
<i>Гальцова С. А.</i> Кибератаки и их общественная опасность	296
<i>Галямина И. А.</i> Актуальные проблемы использования технологий искусственного интеллекта в раскрытии и расследовании преступлений.....	301
<i>Горбачева А. А.</i> Эволюция киберпреступности: от хакинга до криптоджекинга и deepfake	306
<i>Гусева Е. В.</i> Производство следственных действий с применением искусственного интеллекта	310
<i>Дранникова Е. О.</i> Социальная инженерия в киберпространстве: анализ методов, уязвимостей и мер противодействия	315
<i>Егорова В. С.</i> Использование мессенджеров как средство совершения преступления	320
<i>Еремина А. А.</i> Неправомерный доступ и незаконное использование компьютерной информации: анализ и сравнительная характеристика уголовно-правовых составов.....	325
<i>Ермакова А. С.</i> Использование современных информационно-коммуникационных технологий для развития культуры социального взаимодействия с населением у сотрудников полиции	332
<i>Ермакова П. А.</i> Правовая характеристика «вебкам-индустрии» как преступное явление в интернете	337
<i>Зайцева Е. А.</i> Порядок получения голосовой информации посредством применения мобильной связи и ИТ-технологий	342
<i>Зайчикова Г. А.</i> Современные киберугрозы и их влияние на критическую информационную инфраструктуру	347
<i>Иванова К. Д.</i> Особенности влияния СМИ и масс-медиа на формирование массового сознания	353
<i>Ивлев К. А.</i> Методы цифровой криминалистики в расследовании киберпреступлений	357

<i>Каргин Н. М.</i> Особенности совершения киберпреступлений в сфере финансов	361
<i>Кеслер П. В.</i> Концепция информационной безопасности банковской системы «Совкомбанк» как ключевая стратегия предотвращения преступлений в киберпространстве	368
<i>Козлова А. В.</i> Проблема развития преступности в сети Интернет для правоохранительных органов в Российской Федерации	374
<i>Колесникова Е. А.</i> Проблемы уголовно-правовой оценки преступлений, связанных с использованием систем анонимизации пользователей в сети Интернет	378
<i>Комлева М. А.</i> Меры противодействия преступлениям с использованием технологии дипфейка	382
<i>Кондаков Н. Д.</i> Deerfake-технологии: угрозы и методы обнаружения	386
<i>Коротеев Д. А.</i> Биометрическая аутентификация: преимущества и уязвимости	391
<i>Крестинина А. В.</i> Развитие искусственного интеллекта в России	395
<i>Крутова Д. В.</i> Деятельность правоохранительных органов по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий	399
<i>Крюченкова А. А.</i> Вопросы защиты несовершеннолетних от кибербуллинга	405
<i>Кубков М. А.</i> Социальная инженерия в кибербезопасности	408
<i>Кудрявцев Д. А.</i> Актуальные проблемы противодействия социальной инженерии	412
<i>Куксов В. А.</i> Отдельные особенности информационного противодействия международному проявлению экстремизма оперативными подразделениями органов внутренних дел Российской Федерации в сети Интернет	415
<i>Кузовлева М. А.</i> Профилактика дистанционного мошенничества	418
<i>Лисица А. А.</i> Современные тенденции развития кибербуллинга	425

<i>Лукашенко П. П.</i> Методика расследования дистанционных преступлений, совершаемых с использованием информационно- телекоммуникационных технологий, на онлайн-платформах для размещения объявлений.....	429
<i>Малина А. Г.</i> Социальная инженерия как метод совершения киберпреступлений	435
<i>Мальцева В. А.</i> Правовое регулирование оказания медицинской помощи с применением телемедицинских технологий	439
<i>Маренкова С. В.</i> Коммерческая тайна как вид конфиденциальной информации	443
<i>Наянзин Н. В., Ошманкевич Е. Р.</i> Применение процедур КУС/AML в противодействии преступлениям на криптовалютных биржах: опыт Южной Кореи	446
<i>Руденко М. М.</i> К вопросу о профилактике вовлечения несовершеннолетних в террористическую деятельность с помощью информационных технологий	451
<i>Тамбовцева М. А.</i> Защита корпоративных данных от утечек и взломов	454
<i>Телелейко А. Д.</i> Цифровой рубль в системе социального обеспечения: перспективы внедрения и правовые проблемы	458
<i>Покасов П. А.</i> Социально-педагогическая профилактика криминальных угроз в образовательной среде с помощью информационно-телекоммуникационных технологий	464
<i>Рошка А. А.</i> Использование мобильных устройств при расследовании преступлений	467
<i>Рыкина С. В.</i> Кибербуллинг среди подростков: причины, последствия и профилактика.....	472
<i>Сараев С. К.</i> Современные виды киберпреступлений: классификация и тенденции.....	477
<i>Саржан В. И.</i> Фишинг как угроза основным правам человека и гражданина, способы защиты	481
<i>Малашкевич С. А.</i> Влияние мессенджеров на диверсионную деятельность несовершеннолетних, методы профилактики	485
<i>Собаценок И. А.</i> Даркнет как современная анонимная среда: проблемы правопорядка и способы борьбы с незаконной деятельностью	490

<i>Солодова Ю. С.</i> Роль искусственного интеллекта в обнаружении и расследовании киберпреступлений: отечественный и зарубежный опыт	494
<i>Соломина А. А.</i> Институциональные механизмы признания террористической деятельности в России: экспертные практики МВД России и ФСБ России	498
<i>Суровикин А. Д.</i> Тенденции развития информационной преступности	502
<i>Филонова Д. А.</i> Угрозы безопасности, связанные с развитием технологии блокчейн	507
<i>Фомичев С. А.</i> Киберпреступность как новый вызов в криминалогии	513
<i>Хватова Я. Д.</i> Способы самозащиты граждан от преступлений, совершаемых с использованием методов социальной инженерии	518
<i>Черникова М. В.</i> Возможности использования искусственного интеллекта для управления информационными массивами данных Big data.....	523
<i>Шапаев М. С.</i> Типичные следственные ситуации, складывающиеся на первоначальном и последующем этапах расследования преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, включая сеть Интернет	527
<i>Шибаров Н. А.</i> Теневой интернет: даркнет между угрозой и свободой	534
<i>Широбокова А. А.</i> Налогообложение криптовалюты: проблемные вопросы и пути их решения	538
<i>Янгулбаев Х. Х-Б.</i> Ответственность за киберпреступление в Уголовном кодексе Российской Федерации: аналитический обзор и судебная практика	543

РАЗДЕЛ IV. Использование искусственного интеллекта в борьбе с преступностью в России и зарубежных странах

<i>Буравлева А. К.</i> Борьба с киберпреступностью: сравнение законов о киберпреступности в Саудовской Аравии и США	547
<i>Воротникова И. Г.</i> Киберпреступность как глобальная индустрия и ее экономические последствия	552
<i>Серебрякова О. М.</i> Повышение эффективности мер по предотвращению киберпреступности посредством мониторинга государственной политики	556

<i>Вачаев В. В.</i> Сотрудничество правоохранительных органов стран США и Великобритании в борьбе с киберпреступностью на примере мегаполисов	562
<i>Воробьева Д. С.</i> Противодействие киберпреступлениям	567
<i>Горкина У. Р.</i> Правовые проблемы и меры реагирования на киберпреступность в Канаде	572
<i>Горшенева И. А., Гавриленков И. С.</i> Выявление и предотвращение киберпреступлений: обзор возможностей моделей машинного обучения.....	576
<i>Грунина А. М.</i> Проблема борьбы с киберпреступностью в Сербии: особенности регулирования в сфере информационной безопасности	580
<i>Кольяк А. П.</i> Противодействие преступлениям, совершенным в даркнет: сравнительный анализ в США и России.....	585
<i>Кольшикин М. Л.</i> Кибергигиена: как повысить осведомленность общества в борьбе с киберугрозами	589
<i>Короленко Е. С.</i> Роль искусственного интеллекта в противодействии киберпреступности.....	595
<i>Котцова М. П.</i> Роль международного сотрудничества в борьбе с киберпреступностью в США.....	600
<i>Кравченко В. И.</i> Методы отслеживания транзакций криптовалют при расследовании финансирования преступных организаций	605
<i>Криставчук С. М.</i> Расследование и сбор доказательств по делам о киберпреступлениях	611
<i>Мжельская Г. М., Кунгурцев Т. Е.</i> Противодействие преступлениям в сфере информационных телекоммуникационных технологий в США.....	616
<i>Соломина А. А.</i> Использование геоинформационных систем (ГИС) и криминальной аналитики как метода прогнозирования преступной деятельности	620
<i>Хмирова Е. А., Кузнецова С. А.</i> Опыт Китая в борьбе с киберпреступностью.....	623
<i>Яценко С. И.</i> Противодействие киберпреступности в Великобритании	628

РАЗДЕЛ I. ТРИБУНА РУКОВОДИТЕЛЯ

Пушкарев В. В.¹,
*начальник кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

УЩЕРБ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ: ГЛОБАЛЬНЫЙ АНАЛИЗ НОРМ И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ

Цифровая трансформация размывает традиционные границы, создавая гиперсвязанный мир, в котором физическая и виртуальная сферы неразрывно переплетены. Эта взаимосвязанность, предлагая беспрецедентные возможности для прогресса и инноваций, одновременно расширяет поле атаки и усиливает потенциал системного риска. Преступники, начиная от спонсируемых государством групп и организованных киберпреступников и заканчивая хактивистами и отдельными лицами, все чаще нацеливаются на информационную инфраструктуру для шпионажа, получения финансовой выгоды, нарушения работы и даже деструктивных целей.

Растущая зависимость современного общества от информационной инфраструктуры придает первостепенное значение ее безопасности и устойчивости. Кибератаки, направленные на эти системы, представляют серьезную угрозу, что требует создания надежной правовой базы для предотвращения вредоносной деятельности и обеспечения ответственности. Юридический ответ на эти угрозы имеет решающее значение. Эффективная правовая база необходима не только для сдерживания киберпреступности и наказания виновных, но и для создания основы для международного сотрудничества, реагирования на инциденты и установления норм ответственного поведения в киберпространстве.

Опорной проблемой в этой области права является концептуализация и практическое применение понятия «вред» в контексте информационной инфраструктуры, однако в российском законодательстве этот термин не закреплен, что создает серьезные проблемы в правоприменительной практике. Справедливости ради необходимо отметить, что международные и региональные документы также не содержат конкретных определений ущерба информационной инфраструктуре.

Несмотря на растущие усилия законодателей различных стран, сохраняются значительные трудности с эффективным определением «ущерба информационной инфраструктуре», установлением и доказыванием его в ходе судебных раз-

¹ © Пушкарев В. В., 2025.

бирательств. Анализ иностранных и российских источников, составивших теоретическую базу исследования, наглядно выявил как общие черты, так и различия в правовых подходах к определению «ущерба информационной инфраструктуре». Эти проблемы обусловлены неотъемлемыми характеристиками киберпространства и природой кибератак.

Как обсуждалось ранее, большая часть ущерба, причиняемого кибератаками, неосвязаема и с трудом поддается количественной оценке в традиционных юридических терминах. Ущерб репутации, потеря доверия клиентов, нарушение работы основных служб и подрыв общественного доверия – все это реальные и существенные последствия, но доказать их и оценить в денежном выражении может быть непросто.

Отнести кибератаки на счет конкретных участников крайне сложно. Преступники часто используют сложные методы для сокрытия своей личности и происхождения, что затрудняет установление юридической ответственности. Кроме того, доказать прямую причинно-следственную связь между кибератакой и предполагаемым ущербом может быть непросто, особенно в случаях, связанных с каскадным воздействием или косвенными последствиями.

Темпы технологических изменений в киберпространстве опережают возможности законодательной базы. Постоянно появляются новые формы кибератак и уязвимости, что требует постоянной адаптации законодательства и юридических толкований, именно поэтому определение «вреда» должно быть в достаточной степени рассчитаны на будущее, чтобы охватывать возникающие угрозы.

Киберпреступность по своей сути носит транснациональный характер, часто затрагивая преступников, жертв и инфраструктуру, расположенную в разных юрисдикциях. Это поднимает сложные юрисдикционные вопросы и проблемы в трансграничном правоприменении и судебном преследовании. Ущерб, причиненный в одной юрисдикции, может быть вызван действиями в другой, что еще больше усложняет уголовное преследование и судебное разбирательство.

Традиционные стандарты доказывания могут плохо подходить для цифровой сферы. Цифровыми доказательствами можно легко манипулировать или уничтожать, а установление их подлинности и целостности может оказаться сложной задачей. Потребуется адаптировать правила и процедуры доказывания для эффективного использования цифровых доказательств в делах о киберпреступлениях.

Понятия «ущерб», «серьезный ущерб» или «существенный ущерб» могут варьироваться в зависимости от юрисдикции. Например, CFAA США дают относительно широкие определения, в то время как другие (например, СМА Великобритании, Директива ЕС) подчеркивают порог «серьезности». На подход Китая особое влияние оказывают соображения национальной безопасности, что приводит к более широкому толкованию термина «вред» в этом смысле. Все регионы признают важность защиты критической инфраструктуры, но конкретные секторы, определяемые как «критические», и подходы к регулированию их защиты различаются. Директива ЕС NIS [2] и Сингапурский закон о кибербезопасности [1] содержат более подробные рамки для СИ/OES по сравнению с CFAA США, которые в большей степени применимы к компьютерным преступлениям. Китай

и Вьетнам четко определяют приоритетность национальной безопасности и социальной стабильности в своем законодательстве о кибербезопасности, что потенциально расширяет возможности толкования термина «вред» и уголовного преследования за киберпреступления. Хотя западные юрисдикции, как правило, уделяют больше внимания экономическому ущербу и нарушению работы служб, проблемы национальной безопасности также становятся все более актуальными. В таких условиях согласование юридических определений и стандартов доказывания в различных правовых системах остается серьезной проблемой.

Итак, определение и доказывание «вреда» сопряжено со значительными правовыми и доказательственными трудностями. Цифровая сфера требует более тонкого и расширенного понимания вреда, охватывающего неосознаваемые и системные последствия, которые не всегда поддаются количественной оценке или могут быть сразу заметны. В отличие от традиционных преступлений, которые часто сопряжены с ощутимым физическим ущербом, кибератаки часто наносят нематериальный, каскадный и системный ущерб. Потому, рассматривая ущерб информационной инфраструктуре, необходимо выйти за рамки чисто физической или экономической перспективы и рассмотреть более широкие социальные и функциональные последствия кибератак. То есть в широком смысле, вред информационной инфраструктуре может включать в себя большой спектр негативных последствий, начиная от временного нарушения функционирования информационных систем до серьезных экономических потерь, социальных потрясений и угрозы национальной безопасности. Для целей правового регулирования и правоприменения необходимо сузить данное понятие и выделить конкретные виды вреда, которые подлежат правовой оценке и влекут за собой ответственность. Таким образом, вред информационной инфраструктуре является многоаспектным и требует четкого определения, выделения значимых признаков дефиниции, типологии и выработки методологии оценки для целей уголовного и административного преследования за киберпреступления.

В основу определения должна быть положена классификация видов вреда информационной инфраструктуре.

Наиболее легко поддается количественной оценке экономическая форма ущерба информационной инфраструктуре, включающая финансовые потери из-за сбоев в работе, кражи интеллектуальной собственности, выплаты выкупа, затраты на реагирование на инциденты и восстановление, а также ущерб репутации на рынке.

Нарушение или деградация основных услуг и функциональных возможностей, предоставляемых инфраструктурой, и выражающаяся, например, во временных отключениях или длительных системных сбоях, оказывающих влияние на такие критически важные отрасли, как здравоохранение, транспорт, энергетика и финансы, - относится к операционному ущербу.

Кибератаки на информационную инфраструктуру могут нанести серьезный социальный ущерб. Так, нарушение работы основных служб может привести к неудобствам для населения, беспокойству и даже социальным волнениям. Утечка данных может привести к краже личных данных, нарушению конфиден-

циальности и подрыву общественного доверия к цифровым системам. Дезинформация и кампании по дезинформации, нацеленные на инфраструктуру, могут подорвать управленческие процессы и социальную сплоченность.

Атаки на правительственные сети, избирательные системы и критически важную инфраструктуру образуют политический ущерб и могут быть истолкованы как акты агрессии или принуждения, подрывающие национальную безопасность и международную стабильность. Кибершпионаж и кража данных могут поставить под угрозу национальные интересы и дипломатические отношения.

Постоянная угроза кибератак и возможность стать жертвой киберпреступности могут вызывать психологический ущерб, выраженный в стрессе, тревоге и страхе. Он оказывает сильное влияние на индивидуальное благополучие и доверие общества к цифровым технологиям.

Кибератаки, хотя и не являются прямыми, потенциально могут нанести ущерб окружающей среде. Например, атаки на промышленные системы управления в критически важных секторах инфраструктуры, таких как энергетика или очистка воды, могут привести к загрязнению окружающей среды или истощению ресурсов.

Понимание этих разнообразных аспектов ущерба имеет решающее значение для разработки всеобъемлющей правовой базы, учитывающей весь спектр рисков, связанных с кибератаками на информационную инфраструктуру. Юридическое определение ущерба должно быть достаточно широким и гибким, чтобы охватывать эти многогранные последствия.

Подробный анализ предопределяет градацию вреда в киберпространстве также заключается в различии между материальным и нематериальным ущербом. Под материальным ущербом понимается прямой физический ущерб или экономические потери, которые легко поддаются измерению и количественной оценке. С другой стороны, нематериальный ущерб включает в себя менее заметные и с трудом поддающиеся количественной оценке последствия, такие как ущерб репутации, потеря доверия клиентов, перебои в предоставлении услуг и подрыв общественного доверия.

Традиционные правовые системы зачастую лучше приспособлены для устранения материального ущерба. Доказать финансовые потери или физический ущерб, как правило, проще, чем продемонстрировать ущерб репутации или социальные последствия сбоев в обслуживании. Однако нематериальный ущерб информационной инфраструктуре может быть таким же или даже более значительным, чем материальный. Длительный сбой в работе критически важной инфраструктурной системы, даже без прямого физического ущерба, может иметь далеко идущие и разрушительные последствия для общества.

Правовые рамки должны развиваться для эффективного устранения как материальных, так и нематериальных форм ущерба в киберпространстве. Это требует разработки методологий для оценки и количественного определения нематериального ущерба, а также правовых механизмов для обеспечения возмещения ущерба жертвам такого ущерба. В результате исследования необходимо сформулировать ряд частных выводов.

Во-первых, необходимо разработать достаточно четкое определение «вред информационной инфраструктуре», чтобы обеспечить юридическую определенность для государства, организаций и частных лиц. При этом оно должно быть достаточно широким, чтобы охватывать многогранный характер ущерба, причиняемого кибернетическими объектами, включая нематериальные и системные последствия. Определение должно быть адаптировано к меняющимся киберугрозам и технологическим достижениям.

Во-вторых, необходимо укреплять стандарты доказывания и возможности цифровой криминалистики посредством инвестирования в исследования и разработку передовых инструментов и методов цифровой криминалистики для улучшения возможностей идентификации и атрибуции, а также сбора и анализа цифровых доказательств, адаптировать правила и процедуры доказывания для более эффективного использования цифровых доказательств в делах о киберпреступлениях, содействовать обучению сотрудников правоохранительных органов, прокуроров и судей методам цифровой криминалистики и расследования киберпреступлений.

Список литературы

1. Закон о кибербезопасности Сингапура // URL: <https://www.csa.gov.sg/legislation/cybersecurity-act>.
2. Директива ЕС NIS // URL: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.
3. Константинов А. В., Михайленко Н. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы // Вестник Московского университета МВД России. 2023. № 3. С. 129–132.

Зайцев О. А.¹,

*главный научный сотрудник центра
уголовного, уголовно-процессуального
законодательства и судебной практики
Института законодательства
и сравнительного правоведения
при Правительстве Российской Федерации,
вице-президент Союза криминалистов и криминологов,
доктор юридических наук, профессор,
заслуженный деятель науки Российской Федерации,
почетный работник высшего профессионального
образования Российской Федерации*

ОСОБЕННОСТИ ДОКАЗЫВАНИЯ В ХОДЕ ПРОИЗВОДСТВА ПО УГОЛОВНОМУ ДЕЛУ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Одной из значимых национальных целей развития России на период до 2030 г. является достижение цифровой трансформации, которая объективно обусловила расширение использования современных цифровых платформ и различного рода технологий в доказывании в ходе производства по уголовному делу.

Проведенный анализ судебно-следственной практики показывает наличие проблем в обнаружении, фиксации и использовании в процессе доказывания следов преступления, отраженных в различных электронных документах, сообщениях мессенджеров и письмах электронной почты, цифровых видео- и аудиозаписях.

Верховный Суд Российской Федерации обратил на внимание на данные проблемы и в целях их разрешения в своем Постановлении Пленума от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» дал правоприменителю разъяснения относительно применения положений действующего законодательства, регламентирующего оборот информации и информационных технологий в рамках разбирательства уголовных дел.

В юридической науке в последнее десятилетие осуществляются фундаментальные и прикладные исследования проблем, связанных с применением электронных средств доказывания по уголовному делу:

- определением понятия, видов и классификации электронных доказательств;
- получением компьютерной информации из информационно-телекоммуникационных сетей, а также сведений из информационных систем операторов сотовой связи, электронных носителей информации;

¹ © Зайцев О. А., 2025.

– исследованием мобильных и компьютерных устройств, электронных следов, документов и иных вещественных доказательств [1, с. 149–155; 2, с. 45–51; 3, с. 75–85].

Особое место уделено определению мер, направленных на совершенствование процессуального порядка производства отдельных следственных действий, позволяющих повысить процессуальные гарантии обеспечения прав и законных интересов лиц, вовлеченных в сферу уголовного судопроизводства [4, с. 66–78].

Среди перспективных направлений совершенствования процесса доказывания обстоятельств совершенного преступления можно выделить следующие.

Использование уникальных свойств цифровой информации, позволяющих сохранять, обрабатывать и идентифицировать личность человека, любые предметы, а также осуществлять фиксацию происходящих событий. Это будет способствовать обнаружению причинно-следственных и пространственно-временных связей и взаимосвязей между сопоставляемыми сведениями; получению новых знаний об обстоятельствах преступления, а также о лицах, их совершивших.

Пересмотр правил допустимости доказательств, содержащих электронную информацию или электронные носители информации, в пользу технических гарантий верифицируемости и полезности доказательства. С учетом возможных рисков и деятельности, связанной с установлением обстоятельств совершения преступления, оптимизация уголовно-процессуальной формы должна осуществляться на основе неприемлемости сокращения существующих гарантий получения достоверных сведений, обеспечения прав и законных интересов невластных участников процесса [5, с. 27–38].

Уголовно-процессуальная деятельность по обнаружению, фиксации, хранению и предоставлению цифровой информации настоятельно требует более активного внедрения электронного документооборота в судопроизводство. Протокольная форма оформления не в полной мере может охватить объемы и сложное структурное содержание современных источников компьютерной информации; имеется опасность ее искажения при переносе с технологического источника на бумажный носитель. В свою очередь, в пользу электронного документооборота свидетельствуют его явные преимущества: транспарентность и повышение уровня доступности к правосудию; удобство и эффективность взаимодействия между участниками уголовного судопроизводства без риска потери доказательственной информации и др. В связи с этим предстоит более детально регламентировать процессуальный порядок применения электронных документов в ходе производства по уголовному делу, включая механизм взаимодействия субъектов процесса в рамках использования систем, предусматривающих возможность подачи подобных документов [6, с. 199–207].

В рамках трансформации уголовно-процессуального доказывания нуждается в дальнейшей правовой регламентации использование электронных доказательств в доказывании виновности (невиновности) лица в совершении преступного деяния, а также иных обстоятельств, имеющих отношение к уголовному делу. Предстоит определить содержание электронных доказательств и их место

в системе источников доказательств, процессуальный порядок признания их таковыми, специфику собирания, проверки и оценки в ходе уголовного судопроизводства [7, с. 460–467; 8, с. 132–144].

В перспективе следует расширить круг следственных действий, позволяющих более продуктивно получать доказательственную информацию в электронном формате. В юридической литературе уже высказывались достаточно веские аргументы в пользу необходимости законодательного регулирования возможности проведения онлайн-обыска, допускающего правомерный взлом необходимого цифрового устройства, а также обход средств его защиты в целях получения доказательств в рамках уголовного дела; компьютерного моделирования, оказывающего помощь в установлении новых мест для поиска потенциальных доказательств и др. [9, с. 67–77].

Внедрение информационно-цифровых технологий диктует необходимость конкретизировать компетенцию и полномочия каждого из субъектов уголовно-процессуального доказывания относительно возможностей их применения; предложить новые направления и механизмы реализации правовых отношений; определить пределы дискреции судебно-следственных органов в рассматриваемой сфере деятельности.

Нуждается в дальнейшем всестороннем осмыслении ученых-исследователей допустимость внедрения технологий искусственного интеллекта (далее – ИИ) в уголовное судопроизводство в качестве инструмента собирания, проверки и оценки доказательств [10, с. 98–102].

Возможными направлениями применения ИИ в ходе раскрытия и расследования преступлений являются:

- *использование цифрового профиля* лица (состоящего из регистрационных данных субъектов и объектов в цифровой системе правоотношений, биометрических персональных данных, цифровых идентификаторов личности и окончного оборудования, информационных систем, компьютерных сетей) [11, с. 281–308];

- поиск криминалистически значимой информации в различных базах данных по определенным критериям (в частности, абонентским номерам, MAC-адресам, IP-адресам, IMEI и иным идентификационным модулям, ключевым словам, голосовым, визуальным и иным признакам) [12];

- распознавание лжи, на основе оценки поведения допрашиваемого свидетеля, обвиняемого или иного участника уголовного судопроизводства) [13, с. 240–244].

При этом следует принимать во внимание возможные риски нормативно-правового, технологического и организационного характера, способные изменить сущность источника доказательства, привести к злоупотреблению правом со стороны заинтересованных в исходе дела субъектов уголовно-процессуальных отношений.

В заключение необходимо отметить, что юридической доктрине, законодателю и правоприменителю следует:

- продолжить работу в поиске общих подходов в решении межотраслевых проблем теории и практики доказывания в условиях цифровой трансформации;

определить допустимые границы объединения информационно-технологического, криминалистического знания с классической моделью судебных доказательств;

создать эффективные механизмы использования электронной информации в процессе доказывания. При этом важно принять во внимание уже имеющийся опыт зарубежных государств в части использования электронной информации в качестве доказательств по уголовному делу [14, с. 42–57].

Список литературы

1. Пушкарев В. В. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере // Вестник экономической безопасности. 2024. № 5. С. 149–155.
2. Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. № 3. С. 45–51.
3. Валов С. В. Получение следователем сведений из информационных систем операторов сотовой связи: правовые и организационно-технологические модели // Актуальные проблемы судебной, правоохранительной, правозащитной, уголовно-процессуальной и антикоррупционной деятельности : матер. Междунар. науч.-практ. конф. / отв. ред. В. А. Семенцов. Ч. 1. Краснодар, 2024. С. 75–85.
4. Малышева О. А., Самсонов П. А. Применение следователем информационно-коммуникационных технологий при производстве следственных действий: риски и пути их преодоления // Журнал российского права. 2024. Т. 28. № 2. С. 66–78.
5. Гаврилин Ю. В., Победкин А. В. Модернизация уголовно-процессуальной формы в условиях информационного общества // Труды Академии управления МВД России. 2019. № 3. С. 27–38.
6. Александров А. С., Андреева О. И., Зайцев О. А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского государственного университета. 2019. № 448. С. 199–207.
7. Пушкарев В. В. Уголовное преследование лиц, совершивших киберпреступления: опыт, проблемы и пути их преодоления // Предупреждение преступлений органами внутренних дел в свете современных угроз национальной безопасности. М. : Московский университет МВД России имени В.Я. Кикотя, 2019. С. 460–467.
8. Никурадзе Н. О. «Электронные доказательства» в уголовном процессе: о целесообразности правового регулирования // Журнал российского права. 2024. Т. 28. № 4. С. 132–144.
9. Зуев С. В., Зазулин А. И. Цифровой УПК: новая концепция развития права // Правопорядок: история, теория, практика. 2024. № 1. С. 67–77.
10. Муратов К. Д., Муратова Н. Г. Процессуальная и криминалистическая модель применения технологий искусственного интеллекта при проверке сообщений о преступлении в случае передачи собственником средств и систем фото-

и видеонаблюдения изображений гражданина (научное мнение по п. 5 ч. 1 ст. 4 Федерального закона от 24 апреля 2020 г. № 123-ФЗ) // Вестник экономики, права и социологии. 2020. № 2. С. 98–102.

11. Зайцев О. А., Пастухов П. С. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. 2022. Вып. 56. С. 281–308.

12. Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений : монография. М., 2021.

13. Новикова К. С. Искусственный интеллект как элемент электронного правосудия: смарт-решение и электронные весы правосудия // Образование и право. 2022. № 3. С. 240–244.

14. Зайцев О. А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 4. С. 42–57.

15. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / [В. В. Пушкарев, А. В. Константинов, В. Б. Вехов и др.]. М. : Ай Пи Ар Медиа, 2025.

Тисен О. Н.¹,

*начальник юридического управления Росфинмониторинга,
доктор юридических наук*

ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ: СЛЕДСТВЕННАЯ И СУДЕБНАЯ ПРАКТИКА

Официальная статистика совершения преступлений с использованием криптовалют в России, как и в большинстве стран мира, отсутствует. Однако число фактов зарегистрированных деяний этой категории не может отражать реальную картину в силу высокой анонимности криптовалют, децентрализованности их выпуска и обращения, отсутствия единых механизмов противодействия использованию виртуальных активов [1] в противоправных целях. Применяемые во всем мире методики на сегодняшний день не позволяют оказывать эффективное противодействие использованию криптовалют в противоправных целях, выявлять, пресекать и доказывать такие преступления.

На 01.05.2025 в уголовном и уголовно-процессуальном законодательстве России нормы о криптовалюте, признании ее имуществом для целей уголовного судопроизводства, особенностях их ареста и конфискации отсутствуют. Однако результаты анализа судебной практики [2] подтверждают, что в большинстве случаев суды стали рассматривать криптовалюты в качестве предмета преступлений различных категорий уже более 10 лет назад. В ГАС «Правосудие» содержится свыше 1500 решений по делам этой категории [3].

Преступления, совершенные с использованием криптовалют, можно условно разделить на три группы:

Преступления, в которых криптовалюта использовалась для конспирации преступной деятельности и/или в качестве средства платежа [4] (легализация преступных доходов, преступления коррупционной и экономической направленности и т. д.).

Фактически с использованием криптовалют может быть совершено любое преступление, предполагающее получение дохода или использование средств платежа.

Преступления, в которых криптовалюта является предметом преступного посяательства (кражи, мошенничество, грабежи, разбой и т. д.) [5];

Преступления, связанные со злоупотреблениями при совершении майнинга, которые на практике связаны с хищением электроэнергии (ст.ст. 165, 159 УК РФ) [6].

Криптовалюта используется преступниками, прежде всего, в целях конспирации преступной деятельности, а также уклонения от ареста и конфискации преступных активов.

¹ © Тисен О. Н., 2025.

Как правило, преступления, совершенные с использованием криптовалют, выявляются при расследовании уголовных дел о деяниях, совершенных «традиционным» способом в ходе проведения следственных действий и ОРМ: обыска, осмотра места происшествия, допросов, осмотра вещественных доказательств и т. д. Исключения составляют преступления, в которых криптовалюта была предметом преступного посягательства, которые чаще всего выявляются после заявления потерпевших.

За 15 лет существования технологии распределенного реестра отношения в этой сфере существенно трансформировались. Появились миксеры, тумблеры и анонимайзеры, позволяющие скрыть следы связи конкретного владельца с транзакциями, сформировалась развитая инфраструктура провайдеров услуг в сфере виртуальных активов (далее – ПУВА) [1], в том числе работающих в теневом секторе, а количество криптовалют многократно увеличилось.

Резкий рост фактов использования криптовалют для совершения преступлений во всем мире был отмечен в 2017 г., что обусловлено значительным возрастанием стоимости самых распространенных криптовалют. В последние годы незаконный оборот товаров и услуг, запрещенных и/или ограниченных в гражданском обороте (сбыт наркотиков, оружия и т. д.), как правило, осуществляется с использованием криптовалют.

Среди преступлений против собственности, предметом которых была криптовалюта, выявлены не только факты кражи и мошенничества, но и грабежа и разбоя.

Так, согласно приговору Петроградского районного суда, г. Санкт-Петербурга от 20.12.2021, осужденный по п. «б» ч. 3 ст. 161 УК РФ признан виновным в открытом хищении криптовалюты, которое выразилось в переводе потерпевшим на криптокошелек осужденного криптовалюты под угрозой применения насилия [7].

Приговором Всеволожского городского суда Ленинградской области от 08.04.2019 признан виновным А. в совершении разбоя с применением предмета, используемого в качестве оружия, в ходе которого была похищена криптовалюта потерпевшего [8].

Высокая стоимость самых распространенных криптовалют побуждает лиц даже к совершению преступлений против личности с целью завладения виртуальными активами. Так, приговором Петродворцового районного суда Санкт-Петербурга от 05.04.2021 В. признан виновным, помимо прочего, в покушении на похищение человека с угрозой применения насилия, опасного для жизни и здоровья с применением оружия, из корыстных побуждений; в покушении на умышленное причинение смерти другому человеку; в требовании передачи чужого имущества под угрозой применения насилия, в особо крупном размере. Согласно приговору суда, В. вымогал у потерпевшего 10 биткойнов, пытался его похитить и убить с целью получения его имущества в криптовалюте [9].

Выявлены факты совершения должностных и коррупционных преступлений с использованием криптовалюты [10].

На 01.05.2025 криптовалюта и другие виртуальные активы на законодательном уровне не признаны имуществом для целей применения УК РФ. Статус цифровой валюты как имущества закреплен в законодательстве о банкротстве, об исполнительном производстве, о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма [11].

Имевшая место в течение нескольких лет практика оправдания, исключения из объема предъявленного обвинения, возвращения судами прокурорам уголовных дел фактически в связи с отсутствием в законодательстве норм, относящих криптовалюту к имуществу для целей применения УК РФ, существенно изменилась в 2021 г.

Так, П. П. и П. Е. было предъявлено обвинение в том, что они под угрозой применения насилия похитили у потерпевшего Ш. 5 млн рублей, а также предъявляли требование о совершении транзакций криптовалюты на находящихся в их пользовании криптокошельки. В результате под давлением потерпевший перевел обвиняемым криптовалюту на общую сумму свыше 55 млн рублей. По приговору Петроградского районного суда Санкт-Петербурга от 30.06.2020 П. П. осужден по ч. 2 ст. 325 УК РФ, п. «б» ч. 3 ст. 163 УК РФ, П. Е. – по п. «б» ч. 3 ст. 163 УК РФ. При этом суд исключил из объема предъявленного обвинения похищенную осужденными криптовалюту на общую сумму свыше 55 млн 197 тыс. рублей. Сославшись на информационное письмо Банка России от 27.01.2014 «Об использовании при совершении сделок «виртуальных валют», а также на положения статей 128 и 209 ГК РФ, суд сделал вывод о том, что криптовалюта не может являться предметом преступления против собственности в связи с отсутствием у нее правового статуса, не является объектом гражданского права и средством платежа. Суд апелляционной инстанции в определении от 23.11.2020 согласился с позицией суда первой инстанции, указав на несоответствие криптовалюты требованиям, предъявляемым к электронным денежным средствам [12].

Отменяя решения судов первой и апелляционной инстанций по представлению прокурора, Судебная коллегия по уголовным делам Третьего кассационного суда общей юрисдикции указала, что ст. 128 ГК РФ относит к имущественным правам, в том числе, цифровые права. В соответствии с примечанием к ст. 158 УК РФ предметом хищения выступает имущество, противоправное безвозмездное изъятие и обращение которого в пользу виновного причиняет ущерб собственнику или иному владельцу имущества. «Таким образом, судам следовало учесть, что цифровая валюта могла быть принята в качестве средства платежа, не являющегося денежной единицей иностранного государства и международной денежной или расчетной единицей. По своей сути основным отличием криптоденег от денег является только способ их возникновения, а поскольку понятие криптовалюты не закреплено законодательно, обозначение ее как иного имущества в обвинении, предъявленном осужденным, являлось допустимым. В этой связи ссылки суда на информационное письмо Банка России об отсутствии обеспечения по «виртуальным валютам», не может свидетельствовать об отсутствии предмета преступления по смыслу примечания к ст. 158 УК РФ, поскольку криптовалюта использовалась и используется как средство платежа, инвестиций и

накопления сбережений, т. е. представляет экономический интерес, а также имеет материальную ценность» [13].

Ранее пробелы правового регулирования в части признания криптовалюты имуществом для целей УК РФ нередко влекли за собой вынесение правоохранительными органами постановлений об отказе в возбуждении уголовных дел и являлись поводом для оспаривания сторонами состоявшихся судебных решений [14].

После удовлетворения представления прокурора и вынесения Третьим кассационным судом общей юрисдикции кассационного определения от 24.06.2021 № 77-1411/2021 следственная и судебная практика изменилась. Суды все чаще стали признавать криптовалюту предметом хищений [15], в том числе кражи, мошенничества [16], грабежа [7], разбоя [8], вымогательства [17] и других преступлений [7, 8, 13], а количество направленных в суды уголовных дел этой категории существенно увеличилось.

В определении от 21.12.2023 № 77-5316/2023 Восьмой кассационный суд общей юрисдикции указал, что «вопреки доводам кассационной жалобы, суждения осужденного о невозможности признания похищенной у потерпевшего криптовалюты предметом хищения основаны на субъективном мнении и не свидетельствуют о наличии оснований для отмены или изменения состоявшихся судебных решений. Выводы судебных инстанций о признании похищенных у потерпевшего биткоинов (криптовалюты) предметом хищения, со ссылкой на соответствующие нормативные акты, судебная коллегия признает верными, аргументированными и обоснованными» [18].

В кассационном определении от 06.06.2023 по делу № 77-1296/2023 Третий кассационный суд общей юрисдикции обратил внимание на то, что «отсутствие законодательного регулирования криптовалюты в виде «биткоинов», «дигибайтов», «битшейресов» и оценки их стоимости в законодательстве РФ, на что ссылается сторона защиты, не исключает квалификации действий по их противоправному безвозмездному изъятию и обращению в свою пользу как хищения, поскольку они имеют определенную имущественную ценность [7].

На сегодняшний день разъяснения Верховного Суда Российской Федерации о статусе криптовалюты в уголовном судопроизводстве опубликованы только в части их использования при совершении преступлений, предусмотренных статьями 174 и 174.1 УК РФ. Согласно постановлению Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» [19], предметом преступлений, предусмотренных статьями 174 и 174.1 УК РФ, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления (абзац введен 26.02.2019). Таким образом, предметом легализации преступных доходов согласно постановлению Пленума ВС РФ № 32 является не криптовалюта, а денежные средства, преобразованные из нее.

В последние годы суды рассматривают криптовалюту как «иное имущество» [20], в том числе при рассмотрении гражданских и арбитражных дел [21]. К примеру, в нескольких апелляционных определениях Московский городской суд прямо указал, что: «...криптовалюта не может быть расценена судом применительно к ст. 128 ГК РФ иначе как иное имущество» [22]. Криптовалюта – разновидность цифровой валюты [23]. В ряде решений ВС РФ криптовалюта и цифровая валюта рассматриваются как тождественные понятия и эти дефиниции приводятся в скобках как равнозначные [24].

Обосновывая вывод о том, что криптовалюта является иным имуществом, суды чаще всего приводят следующую формулировку:

Согласно ст. 128 ГК РФ к объектам гражданских прав относятся вещи (включая наличные деньги и документарные ценные бумаги), иное имущество, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права); результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага.

В соответствии с ч. 3 ст. 1 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.

Таким образом, действующее законодательство относит к объектам гражданских прав не только наличные деньги и безналичные денежные средства, но иное имущество, к которому относится, в частности, цифровая валюта, способная в силу закона выступать в качестве средства платежа и потому, соответственно, имеющая определенную имущественную ценность и стоимостный эквивалент, который также может быть определен и выражен в деньгах» [25].

«...Признание криптовалюты «иным имуществом» не противоречит ст. 128 ГК РФ, в том числе в редакции закона, действующего на момент совершения преступления, учитывая, что возможный перечень такого имущества не являлся и не является закрытым [7].

Выявление и доказывание преступлений, совершенных с использованием криптовалют, имеют специфические особенности, требуют специальных знаний и владения методиками, отличными от применяемых при производстве по иным категориям дел.

В уголовно-процессуальном законодательстве отсутствуют специальные нормы, закрепляющие особенности производства по делам анализируемой категории. Однако, действующие нормы применимы, в том числе, для придания статуса доказательств электронным следам, оставшимся от преступлений, совершенных с использованием криптовалют.

Специфика выявления и доказывания таких деяний заключается в следующем:

- сложность установления факта совершения преступлений с использованием криптовалют. Как правило, такие деяния устанавливаются в ходе расследования преступлений, совершенных традиционными способами, конспирация которых осуществлялась в том числе путем использования виртуальных активов;
- проблематичность, а иногда невозможность установления владельца криптокошелька;
- распространенность деятельности ПУВА вне поля правового регулирования, непроведение верификации клиентов и несоблюдение принципов КУС и AML, что затрудняет, а иногда исключает получение правоохранными органами и ПФР сведений о владельцах криптокошельков, арест и конфискацию криптовалюты;
- использование преступниками ПУВА, находящихся в других юрисдикциях, что усложняет получение необходимой информации в силу сложностей при исполнении международных запросов о правовой помощи между некоторыми странами;
- отсутствие реальных адресов и анонимность владения ПУВА, нахождение их в третьих странах;
- использование преступниками средств анонимизации и шифрования;
- создание нового криптокошелька для совершения каждой преступной транзакции;
- сложности установления стоимости криптовалют по курсу национальной валюты на день совершения преступления, характера и размера вреда, причиненного преступлением;
- проблематичность, а иногда невозможность ареста и конфискации криптовалюты, отмены транзакции, обращения в доход государства виртуальных активов, добытых преступным путем;
- неурегулированность в большинстве стран процессуальных особенностей обнаружения, закрепления, изъятия электронных и иных следов преступлений, совершенных с использованием виртуальных активов;
- недостаточное владение должностными лицами компетентных органов знаниями и навыками выявления, пресечения и расследования рассматриваемых преступлений.

Методика доказывания преступлений, совершенных с использованием криптовалют, зависит от сложившейся следственной ситуации и поведения подозреваемого/обвиняемого:

- подозреваемый/обвиняемый сотрудничает со следствием;

– подозреваемый/обвиняемый отказывается от сотрудничества с правоохранительными органами.

В практике повсеместно встречаются случаи отказа привлеченного к уголовной ответственности содействовать конфискации, аресту и возврату криптовалюты, полученной преступным путем или предназначенной для совершения преступлений. Нередко виртуальные активы остаются у преступников даже после постановления в отношении них обвинительного приговора и назначения им наказания в виде реального лишения свободы.

Как правило, доказательствами по уголовным делам о преступлениях, совершенных с использованием криптовалют, помимо иных, судами признаются:

- результаты осмотра электронных устройств;
- заключения различных видов экспертиз (прежде всего, компьютерных), объектами которых являлась информация о владении и использовании криптовалюты, содержащаяся на электронных устройствах;
- результаты осмотра и экспертизы холодного/аппаратного криптокошелька;
- результаты осмотра информации об истории и характере криптовалютных транзакций, совершаемых в преступных целях;
- показания специалиста, разъясняющего характер информации о транзакциях, сведения о криптокошельке и т. д.;
- показания эксперта, участвовавшего при производстве экспертиз электронных устройств, изъятых у подозреваемого/обвиняемого;
- ответы ПУВА, которыми пользовались подозреваемые/обвиняемые, на запросы правоохранительных органов и ПФР, и результаты их осмотра;
- ответы компании, предоставляющей услуги мобильной связи, на запросы о том, на кого зарегистрированы номера телефонов, к которым привязаны криптокошельки;
- результаты осмотра телефонной книги в смартфоне подозреваемого на предмет наличия сведений о возможной причастности к преступлению;
- сведения о геолокации/биллинге фигурантов, использующих номера телефонов, к которым привязан криптокошелек;
- информация о переписке и телефонных переговорах, в которых содержались данные, относящаяся к совершенному преступлению;
- сведения о времени и месте удаленного подключения к информационным ресурсам, используемом для этого оборудовании, в том числе модели, сетевом и физическом адресе, серийном номере электронного устройства;
- результаты осмотра контента в социальных сетях, группах в мессенджерах, в которых размещалась информация об использовании криптовалютного адреса/кошелька;
- результаты осмотра переписок организатора финансирования терроризма, отправителя и получателя средств;
- протоколы допросов подозреваемого/обвиняемого, свидетелей об обстоятельствах совершения преступлений;

- результатах обыска/выемки, осмотра места происшествия, в ходе которых были найдены носители с указанием приватного ключа (записка, блокнот, тетрадь и т. д.);
- сведения об IP, IMEI и MAC-адресах электронных устройств, с которых осуществлялся доступ к криптокошелькам;
- результаты обыска/выемки в офисе ПУВА, допросов его сотрудников;
- информация из кредитных организаций о финансовых операциях с деньгами, в которые была конвертирована криптовалюта, и результаты ее осмотра;
- выписки по банковским и электронным счетам, принадлежащим подозреваемым/обвиняемым;
- протокол осмотра сведений о банковских операциях, в ходе которого обвиняемый указал на поступления, являющиеся результатом конвертации криптовалюты, добытой преступным путем, в фиатные деньги;
- результаты бухгалтерских и иных экспертиз, произведенных с целью анализа фиатных финансовых операций фигурантов;
- фото- и видеоматериалы, на которых зафиксировано обналичивание средств;
- результаты экспертиз по извлечению информации из заблокированных электронных устройств;
- иные доказательства.

Все действия должностных лиц с криптовалютой должны быть пошагово зафиксированы в протоколе с приложением фототаблицы и (или) видеозаписи, в том числе реквизиты криптокошельков и криптовалюты, наименование и другие сведения о криптобирже/обменнике, информация о транзакциях.

Важно учитывать особенности установления времени совершения транзакций, которое по делам о преступлениях против собственности и ряду иных категорий является временем совершения преступления, входящем в предмет доказывания согласно ст. 73 УПК РФ. Время совершения преступления устанавливается путем изучения транзакций хеш-кода пользователями и их осмотра. В открытых блокчейнах представлена информация о точном времени осуществления операции. При фиксации факта совершения транзакций необходимо обращать внимание на точность указания в процессуальных документах сведений о них. Важно учитывать, что время в блокчейне указывается по Гринвичу (среднее солнечное время меридиана, проходящего через прежнее место расположения Гринвичской королевской обсерватории около Лондона). Время по Гринвичу составляет: – 3 часа от часового пояса Москвы и Минска; + 6 часов от часового пояса Астаны и Бишкека; +5 часов от часового пояса Ашхабада, Душанбе и Ташкента. Неточности при указании времени совершения транзакции могут повлечь за собой искажение обстоятельств преступления, возникновение/опровержение алиби и существенно отразиться на доказывании [26].

Без обнаружения, фиксации и придания статуса доказательств электронно-цифровым следам, оставленным в результате совершения преступлений этой категории, в ходе предварительного расследования, их выявление и доказывание

возможно исключительно в случае содействия подозреваемого/обвиняемого [27].

Следы совершения преступлений с использованием криптовалют могут сохраняться на электронных устройствах, находящихся в пользовании подозреваемого/обвиняемого: смартфонах, планшетах, компьютерах. Впоследствии они подлежат осмотру в рамках ОРМ и/или следственных действий и в процессе производства компьютерной экспертизы.

Для документирования факта совершения преступлений с использованием криптовалют, их последующего ареста и конфискации, помимо традиционных следственных действий и оперативно-розыскных мероприятий необходимо отследить транзакцию. При этом в целях дальнейшего использования полученной информации в качестве доказательства по уголовному делу все действия оперативно-полномоченного/следователя должны быть пошагово зафиксированы в протоколе с приложением фототаблицы и (или) видеозаписи.

В целях закрепления электронных следов совершения преступления с использованием виртуальных активов важно скопировать информацию с электронных устройств лиц, причастных к совершению преступления. Копирование информации возможно, как с изъятием, так и без изъятия электронных устройств.

Особенности изъятия электронных носителей информации при производстве следственных действий закреплены в ст. 164.1 УПК РФ. Согласно ч. 2, 3 ст. 164.1 УПК РФ, электронные носители информации изымаются в ходе производства следственных действий с участием специалиста, которым может быть произведено копирование содержащихся на них сведений по решению следователя, по ходатайству законного владельца или обладателя. С учетом возможности дистанционного перевода криптовалюты на подконтрольный подозреваемому/обвиняемому криптокошелек, передача участникам уголовного судопроизводства и иным лицам скопированной информации с изымаемых электронных устройств по рассматриваемой категории уголовных дел нецелесообразна.

В ходе осмотра электронных устройств может быть обнаружена важная информация, имеющая решающее значение для привлечения лица к уголовной ответственности, обеспечения возможности ареста и конфискации криптовалюты. Так, в ходе осмотра телефонов, изъятых у подозреваемого в незаконном сбыте наркотических средств в составе ОПГ, была обнаружена программа, предназначенная для хранения и накопления криптовалюты различных видов (криптокошельки) [28].

В ходе осмотра электронных устройств фиксируются электронные следы, указывающие на:

- использование владельцем криптовалютных кошельков и сервисов;
- письма с криптобирж и обменников, подтверждающие открытие криптокошелька и его использование;
- сведения о транзакциях;
- наличие в истории браузера поисковых запросов криптовалютной тематики;
- письма из службы поддержки криптобирж и обменников;

- следы хранения сведений об открытых и закрытых ключах (в устройствах могут храниться файлы с сохраненными паролями доступа, открытыми и приватными ключами);
- переписку подозреваемого/обвиняемого с соучастниками преступления или потерпевшими, участниками террористических организаций;
- факты размещения в свободном доступе, а также в закрытых группах социальных сетей и мессенджеров постов о сборе средств на криптовалютные кошельки или совершенных транзакциях;
- иные сведения, свидетельствующие о совершенном преступлении, позволяющие установить связь конкретного лица с криптокошельком, обеспечить арест, замораживание (блокирование) криптовалюты.

Следы отдельных операций с криптовалютой могут быть выявлены на этапе конвертации. Связующим звеном между кредитной организацией, с помощью которых злоумышленники получают возможность получить фиатные деньги из криптовалюты, являются криптовалютные биржи и обменники, в которые можно послать запрос.

С учетом того, что информация о транзакциях криптовалюты не относится к сведениям, составляющим банковскую тайну (по смыслу ст.ст. 29 и 165 УПК РФ) в России применяются следующие способы получения информации от криптобирж и обменников:

- получение правоохрнительными органами необходимых сведений из криптобирж и обменников путем направления запроса соответствующему ПУВА, многие из которых, несмотря на отсутствие закрепления обязанности соблюдать требования ПОД/ФТ в нормах права, осуществляют верификацию пользователей и сотрудничают с правоохрнительными органами в целях противодействия преступлениям;
- путем проведения оперативно-розыскных мероприятий или следственных действий. Такой способ применяется в случае отказа ПУВА сотрудничать с правоохрнительными органами;
- направление по закрытым каналам связи международного запроса в ПФР страны, в которой зарегистрирован ПУВА, через Росфинмониторинг;
- направление запроса об оказании международной правовой помощи компетентным органом одного государства другому. На практике запросы, направляемые правоохрнительными органами в таком порядке, исполняются гораздо дольше запросов, направляемых правоохрнительными органами в ПУВА напрямую или по закрытым каналам связи подразделениями финансовой разведки.

В случае отказа незарегистрированных или работающих в отсутствие правового регулирования ПУВА предоставлять сведения о владельцах криптокошельков, на практике раскрытие преступления, совершенного с использованием виртуальных активов, иногда становится невозможным.

Заключение досудебных соглашений о сотрудничестве по делам о преступлениях, совершенных с использованием криптовалют, – распространенная практика в последние годы [29].

В России криптобиржи и обменники пока не отнесены к субъектам ПОД/ФТ, не обязаны проводить верификацию клиентов, предоставлять информацию о них уполномоченным органам и фактически пока работают вне поля правового регулирования. Нередко установление даже самого факта совершения преступлений с использованием криптовалюты на практике становится возможным только благодаря сотрудничеству привлеченного к уголовной ответственности.

Закон не запрещает заключать досудебное соглашение о сотрудничестве одновременно с несколькими обвиняемыми в рамках одного уголовного дела в форме предварительного следствия, что дает возможность получить больше информации в целях изъятия, ареста и конфискации криптовалюты и фиатных средств, конвертированных из нее, в рамках уголовного судопроизводства.

В целях обнаружения и фиксации электронных следов, позволяющих установить и доказать факт использования виртуальных активов для совершения преступлений, обнаруженные электронные устройства направляются на компьютерную экспертизу.

Нередко в СМИ сообщается о примерах ареста и конфискации криптовалюты. Однако в реальности чаще всего речь идет о проведении оперативно-розыскных мероприятий и следственных действий, в результате которых криптовалюта под контролем правоохранительных органов была конвертирована в фиатные деньги и переведена на подконтрольный сотрудничающему с правоохранительными органами лицу банковский счет, средства на котором были арестованы по решению суда в порядке, предусмотренном ст. 115 УПК РФ. Фактически арест на практике накладывается судом не на криптовалюту, а на фиатные деньги, в которую была конвертирована криптовалюта [30].

Анализ правоприменительной практики показывает, что аресту криптовалюты всегда предшествует обширная исследовательская работа.

В связи с отсутствием централизованного органа, выпускающего децентрализованную криптовалюту, на сегодняшний день существует только два способа обеспечить изъятие, блокировку, арест и конфискации децентрализованной криптовалюты:

Взаимодействие с ПУВА.

Физический доступ компетентных органов к криптокошельку путем изъятия аппаратного криптокошелька или получения приватного ключа (в ходе ОРМ, следственных действий).

Большинство случаев ареста и конфискации криптовалют в мире связаны с изъятием аппаратных криптокошельков, приватных ключей или доступом к кошелькам в результате изъятия электронных устройств фигурантов, посредством которых они совершали преступления с использованием криптовалют.

Фактически арест и последующая конфискации виртуальных активов возможны следующими способами:

- направление компетентным органом требования о замораживании (блокировании), аресте виртуальных активов в ПУВА. Поскольку при использовании услуг централизованных бирж криптовалюта фактически хранится на кошельке биржи, а не клиента, если ПУВА выполняет требования стандартов, применение обеспечительных мер таким способом возможно и результативно;

– перевод криптовалюты из криптокошелька обвиняемого на подконтрольный правоохранительным органам криптокошелек. В ряде стран правоохранительные и судебные органы имеют криптокошельки для ареста, конфискации и залога криптовалют. В Белоруссии и Узбекистане криптовалюты, полученные преступным путем и предназначенные для совершения преступления, переводятся на криптокошелек правоохранительных органов или суда в зависимости от стадии уголовного судопроизводства, на которой происходит этот процесс. В России пока открытие криптокошелька правоохранительными и судебными органами не предусмотрено. После конвертации криптовалюты в фиатные деньги они могут быть обналичены под контролем правоохранительных органов, выданы следователю, после чего на них накладывается арест в установленном законом порядке;

- перевод криптовалюты обвиняемого на аппаратный криптокошелек;
- оставление криптовалют обвиняемых в том же криптокошельке. Важно учитывать, что оставление криптовалюты на кошельке обвиняемого на децентрализованной площадке может привести к их утрате даже в случае, если обвиняемый сотрудничает со следствием. Позиция обвиняемого может измениться, что приведет к выводу преступных активов им самим (если он не находится под стражей или имеет хотя бы вероятную возможность воспользоваться криптокошельком в местах содержания под стражей), соучастниками или иными лицами, имеющими доступ к приватному ключу;
- физическое изъятие аппаратного, десктопного криптокошельков;
- взаимодействие с иными участниками цифровых платформ.

Список литературы

1. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ, июнь 2014 // URL: https://eurasiangroup.org/files/uploads/files/FATF_documents/FATF_Guidances/ROP_Virtualnye_valyuty.pdf.
2. Апелляционный приговор ВС РФ от 13.09.2018 по делу № 127-АПУ18-8; приговоры Советского районного суда г. Красноярск от 02.06.2016 г по делу № 1-457/2016, от 20.02.2017 по делу № 1-41/2017 (1-512/2016), приговор Ленинского районного суда г. Воронежа от 14.08.2017 по делу № 1-181/2017, приговор Ленинского районного суда г. Саранска от 02.05.2017 по делу № 1-87/2017, от 05.06.2017 по делу № 1-100/2017, от 15 июня 2017 г. по делу № 1-102/2017, приговор Metallургического районного суда г. Челябинска от 15.06.2017 по делу № 1-355/2017, приговор Октябрьского районного суда г. Саранска от 08.12.2017 по делу № 1-301/2017, приговор Советского районного суда г. Челябинска от 16.06.2018 по делу № 1-297/2018, приговор Ялтинского городского суда Республики Крым от 30.08.2017 по делу № 1-337/2017.
3. ГАС «Правосудие» // URL: ej.sudrf.ru.
4. Определения Первого кассационного суда общей юрисдикции от 20.01.2022 № 77-553/2022, от 15.07.2021 № 77-2229/2021, от 08.07.2021 № 77-2173/2021, 01.06.2021 № 77-1947/2021, от 20.05.2021 № 77-1371/2021; определение Шестого кассационного суда общей юрисдикции от 14.07.2021

№ 77-3233/2021; кассационное определение Третьего кассационного суда общей юрисдикции от 27.01.2022 № 77-229/2022.

5. Кассационные определения Третьего кассационного суда общей юрисдикции от 06.06.2023 по делу № 77-1296/2023, от 01.07.2021 по делу № 77-1255/2021, от 24.06.2021 № 77-1411/2021.

6. Постановление Пятого кассационного суда общей юрисдикции от 17.05.2023 № 77-751/2023; Кассационное определение Третьего кассационного суда общей юрисдикции от 13.09.2022 № 77-2407/2022; Постановление Восьмого кассационного суда общей юрисдикции от 17.08.2022 № 77-3554/2022.

7. Кассационное определение Третьего кассационного суда общей юрисдикции от 06.06.2023 по делу № 77-1296/2023.

8. Кассационное определение Третьего кассационного суда общей юрисдикции от 01.07.2021 по делу № 77-1255/2021.

9. Кассационное определение Третьего кассационного суда общей юрисдикции от 02.06.2022 по делу № 77-1578/2022.

10. Кассационное определение Третьего кассационного суда общей юрисдикции от 27.01.2022 № 77-229/2022.

11. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

12. Приговор Петроградского районного суда г. Санкт-Петербурга от 30.06.2020 по делу № 1-95/2020; апелляционное определение Санкт-Петербургского городского суда от 23.11.2020 № 22-5295/2020.

13. Кассационное определение Третьего кассационного суда общей юрисдикции от 24.06.2021 № 77-1411/2021.

14. Апелляционные определения Санкт-Петербургского городского суда от 23.11.2020 по делу № 22-5295/2020, от 04.03.2020 по делу № 22-106/2020; определение Шестого кассационного суда общей юрисдикции от 09.09.2020 № 7У-10543/2020[77-1839/2020. и др.

15. Кассационные определения Третьего кассационного суда общей юрисдикции от 02.06.2022 по делу № 77-1578/2022, от 01.07.2021 по делу № 77-1255/2021, от 24.06.2021 № 77-1411/2021, от 06.06.2023 по делу № 77-1296/2023; приговор от 13.11.2017 по делу № 1-762/2017. Практика Сургутского городского суда Ханты-Мансийского автономного округа – Югры // URL: <https://sudact.ru/regular/court/reshenya-surgutskii-gorodskoi-sud-khanty-mansiiskii-avtonomnyi-okrug-iugra/>; кассационное определение Восьмого кассационного суда общей юрисдикции от 21.12.2023 № 77-5316/2023 и др.

16. Определение Шестого кассационного суда общей юрисдикции от 16.01.2024 № 77-78/2024.

17. Определение Первого кассационного суда общей юрисдикции от 04.06.2024 № 77-1995/2024 (УИД 50RS0028-01-2023-003168-98).

18. Кассационное определение Восьмого кассационного суда общей юрисдикции от 21.12.2023 № 77-5316/2023.

19. Постановление Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Российская газета. № 151. 2015.

20. Определение Восьмого кассационного суда общей юрисдикции от 19.09.2023 № 88-18055/2023, кассационное определение Восьмого кассационного суда общей юрисдикции от 11.07.2024 по делу № 77-2735/2024 (УИД 55RS0004-01-2022-003176-41), определение Первого кассационного суда общей юрисдикции от 04.06.2024 № 77-1995/2024 (УИД 50RS0028-01-2023-003168-98, определение Шестого кассационного суда общей юрисдикции от 16.01.2024 № 77-78/2024. и др.

21. Определение Первого кассационного суда общей юрисдикции от 04.06.2024 № 77-1995/2024 (УИД 50RS0028-01-2023-003168-98, определение Шестого кассационного суда общей юрисдикции от 15.11.2022 № 77-4816/2022; определение Девятого арбитражного апелляционного суда от 17.06.2022 № 09АП-39381/2022 по делу № А40-72476/2021, определение Верховного Суда Российской Федерации от 02.02.2021 по делу № 44-КГ20-17-К7 // URL: http://vsrf.ru/stor_pdf.php?id=1969738/.

22. Апелляционные определения Московского городского суда от 20.10.2022 по делу № 33-41465/2022, от 06.09.2023 по делу № 33-36612/2023.

23. «Цифровой рубль. Доклад для общественных консультаций (октябрь 2020 года)» (утв. Банком России).

24. Определение Третьего кассационного суда общей юрисдикции от 25.10.2023 № 88-20686/2023, кассационное определение Восьмого кассационного суда общей юрисдикции от 11.07.2024 по делу № 77-2735/2024 (УИД 55RS0004-01-2022-003176-41).

25. Определение Четвертого кассационного суда общей юрисдикции от 09.03.2023 по делу № 88-7685/2023, определение Седьмого кассационного суда общей юрисдикции от 07.09.2023 по делу № 88-14946/2023.

26. Тисен О. Н. Отслеживание криптовалютных транзакций в целях расследования преступлений // Уголовный процесс. 2024. № 2. С. 54–60.

27. Тисен О. Н. Установление владельцев криптокошельков, обнаружение и изъятие частных ключей при расследовании уголовных дел. // Уголовный процесс. 2024 № 1. С. 78-84.

28. Апелляционное определение Первого апелляционного суда общей юрисдикции от 21.03.2022 № 55-13/2022.

29. Апелляционное определение Московского городского суда от 09.06.2022 № 10-8888/2022; Апелляционное определение Второго апелляционного суда общей юрисдикции от 07.02.2023 № 55-21/2023; Определение Шестого кассационного суда общей юрисдикции от 14.05.2020 № 77-668/2020 Апелляционное определение Второго апелляционного суда общей юрисдикции от 11.12.2020 по делу № 55-592/2020; Апелляционное определение Московского городского суда от 01.03.2021 по делу № 10-573/2021; Апелляционное определение Московского

городского суда от 01.03.2021 по делу № 10-573/2021; Апелляционное определение Московского городского суда от 09.06.2022 № 10-8888/2022; Приговор Свердловского областного суда от 31.01.2019 по делу № 2-5/2019.

30. Определение Шестого кассационного суда общей юрисдикции от 27.06.2023 № 88-13594/2023, апелляционное определение Московского городского суда от 17.12.2021 № 33-49671/2021, апелляционное постановление Верховного суда Республики Дагестан от 01.10.2019 № 22-1867/2019, апелляционное определение Первого апелляционного суда общей юрисдикции от 21.03.2022 № 55-13/2022.

*Минаков С. С.¹,
заместитель генерального директора
Национального технологического центра
цифровой криптографии,
с.н.с. Академии криптографии Российской Федерации*

О РАЗВИТИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПНОСТИ

Согласно Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», борьба с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, является приоритетной задачей для обеспечения государственной и общественной безопасности. К этим преступлениям относятся: незаконное распространение наркотиков, финансирование терроризма и деятельности недружественных государств, легализация преступных доходов, а также использование цифровых финансовых активов и валют в противоправных целях.

Развитие финансовых технологий, платежных систем и цифровизация экономики привели к появлению электронных средств платежа и цифровых валют, которые активно используются для безналичных расчетов. Однако упрощенный доступ к открытию и использованию безналичных расчетов, а также бесконтрольный оборот электронных средств платежа создают условия для их незаконного использования и несут общественные риски.

Информация и ее доступность играют огромную роль в жизни россиян, что привело к переориентации преступных групп на совершение преступлений в киберпространстве. Особенно активны организованные преступные группы, использующие вредоносное ПО, фишинговые сайты, специальную технику, электронные платформы и колл-центры для массового мошенничества [1–3].

Использование цифровых валют для совершения преступлений, включая отмывание доходов, стало обыденным явлением, что затрудняет выявление и конфискацию цифровой валюты, использованной при совершении экономических преступлений [4, 5].

Согласно статистике, каждое третье преступление совершено с использованием информационно-коммуникационных технологий, либо в информационно-коммуникационной сфере.

Огромный ущерб от правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий в период 2015–2025 гг. потребовал наряду с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации создания и развертывания в Российской Федера-

¹ © Минаков С. С., 2025.

ции отдельной государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий.

Двумя основными функциями новой государственной системы борьбы с ИКТ-преступностью в технологической сфере станет:

- создание специализированной цифровой платформы, обеспечивающей оперативный обмен информацией между правоохранительными органами, Центральным банком Российской Федерации, кредитными организациями, а также операторами связи о сведениях, необходимых для установления обстоятельств противоправных деяний и лиц, их совершивших, с использованием средств мобильной связи, сервисов сети «Интернет» и иных информационных технологий (за исключением компьютерных атак и компьютерных инцидентов);

- формирование и поддержание в актуальном состоянии информационных ресурсов федеральных государственных органов и органов государственной власти субъектов Российской Федерации, осуществляющих выработку и реализацию государственной политики в сфере противодействия противоправным деяниям, организаций, деятельность которых связана со сбором, хранением персональных данных, созданием и функционированием информационной инфраструктуры, оборотом цифровой валюты, кредитно-финансовых организаций, организаций, предоставляющих услуги связи и доступа к сети «Интернет».

К числу таких информационных ресурсов, более 5 лет обеспечивающих качественное информационно-аналитическое обеспечение оперативно-розыскной деятельности [6, 7] правоохранительных органов в сфере борьбы с ИКТ-преступностью относится и банк данных «Дистанционное мошенничество», формируемый (заполняемый) территориальными органами внутренних дел в Главном информационно-аналитическом центре МВД России.

Банк данных «Дистанционное мошенничество» предназначен для систематизации, обработки и анализа сведений (в нем содержится несколько миллионов документов: сведения о средствах связи, о банковских реквизитах, о физических лицах и юридических лицах, интернет-ресурсах, электронных кошельках и средствах платежа), собираемых в рамках расследования уголовных дел о преступлениях, совершенных дистанционным способом с использованием информационно-телекоммуникационных технологий [7].

Развитие средств, имеющихся в ведении ГИАЦ банков данных и внедрение новых, позволяет осуществлять качественную информационную поддержку оперативно-розыскной деятельности, а запланированная модернизация информационных ресурсов предоставляет определенные преференции для органов внутренних дел на пути к повышению уровня защищенности граждан и обеспечению правопорядка в стране [8].

Рост киберпреступности связан не только с развитием информационных технологий, но и с уязвимостью жертв, особенно пожилых людей, подростков и детей, чей недостаток правовой и финансовой грамотности делает их легкой мишенью. Преступники все чаще используют новые методы, пользуясь анонимностью

в сети. Появление новых услуг связи (IP-телефония и виртуальные АТС), с недостаточным регулированием, усугубляет проблему, позволяя злоумышленникам оставаться незамеченными.

Ранее недооцененная область достоверности в информационной безопасности столкнулась с новым типом угроз: угрозой авторству цифровых данных, влекущей репутационные риски и подрыв доверия. Наиболее ярким примером этой угрозы является технология DeepFake [10].

В 2021–2025 гг. резко усилились предпосылки к использованию вариаций угрозы авторства и DeepFake, связанные с тем, что в полной мере при хранении данных в распределенных системах (как и по отношению к передаваемой информации или находящейся на отчуждаемых машинных носителях) средства имитозащиты не применяются вовсе, так как не предусмотрены разработчиками, либо используемые в окружающем людей Интернете вещей реализации алгоритмов криптографически слабы [11]. Также срабатывает эффект новизны проблемы в купе с ригидностью людей, проживших много лет в «аналоговом» мире и системах без дополнительной проверки авторства.

Но можно взглянуть и шире не только в сфере аудио- и видео- подделок. Например, в сети выкладывается какой-либо документ, якобы от автора X, при этом подписанный его электронной подписью. В случае нарушения авторских прав X будет тратить силы и время на доказательство своей непричастности. Также данный вид угроз легко применим к различным цифровым деньгам с распределенным механизмом подтверждения транзакций, например, на основе технологии block chain. Естественно, что операционные системы компьютеров и мобильных устройств защищать пользователей от угрозы авторства пока качественно не могут, что создает серьезные последствия при уголовном преследовании [10].

Криминогенную обстановку серьезно осложняет международная напряженность, в частности деятельность спецслужб недружественных стран и неонацистских группировок под их контролем. Основная часть преступлений связана с транснациональными организованными группами, специализирующимися на мошенничестве, включая хищение персональных данных россиян и использование колл-центров, расположенных в недружественных государствах, для кражи денежных средств у граждан.

В силу глобальности интернета и недостаточного международного сотрудничества правоохранительных органов, преступные группы и отдельные злоумышленники эксплуатируют слабые места в технической, организационной и правовой защите, нанося значительный ущерб как финансовый, так и репутационный, гражданам и организациям России. Несмотря на усилия, добиться необходимого уровня информационной безопасности и правовой защиты пока не удалось.

Список литературы

1. Давыдов В. О. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием

информационно-телекоммуникационных технологий / В. О. Давыдов, И. В. Тишутина // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 81–91.

2. Гончар В. В., Грибкова К. А., Михайленко Н. В. и др. Организация расследования хищений денежных средств из банкоматов : учебное пособие. Казань : Бук, 2021.

3. Минаков С. С., Земскова А. В. Особенности применения инструментальных средств для поиска и документирования компьютерной информации в ходе следственных действий по осмотру // Вестник экономической безопасности. 2023. № 2. С. 74–85.

4. Противодействие преступлениям, совершаемым в сфере оборота криптовалюты / [А. В. Андреев, Д. В. Галиев, В. В. Гончар и др.]. М. : Инфра-М, 2022.

5. Семенихина Т. Н. Проблемные аспекты взаимодействия подразделений ОВД при расследовании мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Полиция и общество: проблемы и перспективы взаимодействия. 2022. № 4. С. 133–138.

6. Кузнецов А. А. Возможности подсистемы ИБД-Ф «Дистанционное мошенничество» в рамках расследования уголовных дел по преступлениям, совершенным дистанционным способом с использованием информационно-телекоммуникационных технологий // Совершенствование уголовно-процессуальных и криминалистических мер противодействия преступности : Материалы международной научно-практической конференции, Омск, 29 ноября 2022 г. Омск : Омская академия МВД РФ, 2023. С. 21–25.

7. Морозова Е. Р. Виды дистанционного мошенничества, особенности их квалификации // Актуальные проблемы предварительного расследования : Сборник научных статей международных научно-практических конференций, Санкт-Петербург, 20 апреля 2021 г. СПб. : Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2022. С. 420–427.

8. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / [В. В. Пушкарев, А. В. Константинов, В. Б. Вехов и др.]. М. : Ай Пи Ар Медиа, 2025.

9. Константинов А. В., Михайленко Н. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы // Вестник Московского университета МВД России. 2023. № 3. С. 129–132.

10. Минаков С. С., Михайленко Н. В. Проблемы обеспечения достоверности технических данных и сведений, сопряженных с выявлением и расследованием инцидентов и преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Вестник экономической безопасности. 2023. № 6. С. 107–112.

11. Минаков С. С. О подходах к оценке стойкости криптографических механизмов информационной безопасности для систем и устройств интернета вещей и искусственного интеллекта вещей в условиях ограничений вычислительных возможностей и объема ключа // Комплексная защита информации : Сборник материалов XXIX научно-практической конференции, СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2024. С. 270–275.

Ярмак К. В.¹,

начальник управления учебно-методической работы

Московского университета

МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

РЕАЛИЗАЦИЯ СТАТУСА БАЗОВОЙ ОРГАНИЗАЦИИ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВОГО СОПРОВОЖДЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Существенное значение в укреплении социальных и экономических связей дружественных стран имеют национальные образовательные организации. Справедливым представляется точка зрения авторов научных работ в сфере интеграционных процессов в мировом образовательном пространстве, которые рассматривают международные образовательные обмены и программы, как важный элемент внешней политики России и других ведущих мировых держав [4]. В свете реализации задач по деболонизации отечественного образования и создания эффективной национальной системы высшего образования актуальным остается решение сложных организационных вопросов.

Образовательная политика любой страны нацелена на интенсификацию его влияния на международной арене. Авторы фиксируют возрастающую роль современных образовательных организаций высшего образования в устойчивости общества и обеспечения прорывного его развития [10].

Структура преступности в пределах исторически сложившегося единого евразийского геополитического пространства имеет свои особенности, которые исследуются криминологами [6] и учеными, анализирующими проблемные аспекты развития эффективного международного сотрудничества стран СНГ в борьбе распространенными видами преступлений [8]. В том числе рассматриваются предпринимаемые меры по повышению эффективности взаимодействия компетентных органов в сфере противодействия киберпреступности [1]. Ученые анализируют состояние преступности в странах СНГ в условиях попыток со стороны западных стран нанести ущерб нашей стране путем ведения против России «войны чужими руками», т. н. прокси-войны. Делается акцент на привлечении государств-членов СНГ в качестве инструмента в борьбе против России, путем внесения разногласий, использования в этих своих целях информационных технологий [2].

На пространстве Содружества Независимых Государств широко распространена такая форма взаимодействия, как координация совместной деятельности базовыми организациями государств – участников СНГ в лице различных образовательных, научно-исследовательских и научно-производственных организаций. Решения о придании такого статуса принимались решениями Совета глав правительств СНГ, Совета министров иностранных дел СНГ, Экономического совета

¹ © Ярмак К. В., 2025.

СНГ, начиная с 1997 г. И если до 2004 г. эти решения принимались не более 1 в год, далее до 2023 г. – от 3 до 7 ежегодно, то в 2024 г. такой статус был присвоен 17 организациям. Всего по различным областям и направлениям сотрудничества функционирует 114 базовых организаций, из которых порядка 90 – организации на территории Российской Федерации. Некоторые вузы обладают статусом двух базовых организаций: Белорусский национальный технический университет в г. Минск, Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан в г. Косшы Акмолинской области, Российский университет дружбы народов имени Патриса Лумумбы, а также Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина» Министерства обороны Российской Федерации в г. Воронеж [3].

Вопросы взаимодействия в рамках реализации статуса базовой организации государств – участников СНГ рассматриваются руководителями учеными, педагогами в рамках научно-представительских мероприятий, находят отражение в публикуемых работах. В том числе данные исследования освещают проблемы обеспечения международной безопасности в странах Содружества через призму его роли в системе международных отношений, поднимают вопросы существующих и прогнозируемых угроз коллективной безопасности на международной арене [7]. Специалисты в области международных отношений и международного права, исследователи процессов укрепления многоуровневого партнерства между странами СНГ делятся своим опытом реализации статуса базовой организации [5].

В списке базовых организаций находятся пять организаций системы Министерства внутренних дел, в числе которых четыре – в Российской Федерации и одна – в Белоруссии (Академия Министерства внутренних дел Республики Беларусь в г. Минске), которая обеспечивает подготовку, повышение квалификации и переподготовку кадров в сфере миграции и противодействия торговле людьми. В числе отечественных образовательных организаций по направлению «Борьба с преступностью» ключевые позиции занимают Академия управления Министерства внутренних дел Российской Федерации, обеспечивающая подготовку руководящего состава для органов внутренних дел (полиции), и НПО «Специальная техника и связь» МВД России, как базовое научно-исследовательское учреждение в области разработки специальных средств (оружия нелетального действия) для правоохранительных органов государств – участников СНГ. Кроме того, по направлению «Противодействию финансовым правонарушениям» в перечень включена Нижегородская академия МВД России.

В соответствии с решением Совета министров иностранных дел СНГ от 5 апреля 2019 г. статус базовой организации государств – участников СНГ по подготовке кадров в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий, по образовательным программам высшего образования и дополнительным профессиональным программам придан Московскому университету МВД России имени В.Я. Кикотя (далее – Университет). Указанным Решением утверждено Положение о базовой организации, которое легло в основу деятельности организации помимо Устава СНГ, международно-

правовой базы и решений различных органов управления СНГ. Университет как базовая организация выстраивает свою деятельность во взаимодействии с СМВД и БКБОП, а также образовательными организациями (учреждениями) государств – участников СНГ.

Отметим, что к перечню основных задач базовой организации, помимо подготовки соответствующих профессиональных кадров и ее научного, учебно-методического, информационного, нормативно-методического обеспечения, относятся и актуальные направления по организации взаимодействия вузов государств, обеспечивающих подготовку кадров в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий, включая обмен опытом по разработке и реализации образовательных и научно-исследовательских программ. Большое внимание уделяется организации совместных научных исследований и проведению научно-представительских мероприятий в рамках установленного направления деятельности в области внедрения современных методов борьбы с кибер-преступлениями. Представляет взаимный интерес обмен информационно-аналитическими материалами, научными трудами и учебно-методической литературой.

В настоящее время утвержден состав рабочей группы Университета по координации деятельности базовой организации, ведется активная работа по созданию совещательного органа из представителей вузов государств – участников СНГ.

Ежегодно в интересах правоохранительных и других компетентных органов иностранных государств в Университете осуществляются выпуски иностранных специалистов. Молодые специалисты направляются для дальнейшего прохождения службы в Министерствах внутренних дел Азербайджана, Белоруссии, Республики Казахстан, Киргизской Республики, Республики Таджикистан, Туркменистана, Республики Узбекистан.

В 2019–2024 гг. в целях подготовки иностранных специалистов в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий Университетом реализуется образовательная программа по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, специализация: Технологии защиты информации в правоохранительной сфере. Учитывая специфику подготовки технических специалистов, образовательный процесс направлен на формирование трех уровней компетенций: необходимых для решения технических задач; в сфере общей методологии защиты информации; для защиты информации в правоохранительной деятельности.

На постоянной основе обеспечивается модернизация и актуализация образовательных программ за счет введения новых дисциплин и практик. Кроме того, для подготовки сотрудников компетентных органов иностранных государств разработан проект новой образовательной программы по специальности 40.05.01 Правовое обеспечение национальной безопасности специализация Уголовно-правовая, направленность образовательной программы – Расследование преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Данная образовательная программа подразумевает юридическую квалификацию выпускника.

Формирование актуального набора компетенций осуществляется на специализированной материально-технической базе учебно-научного комплекса информационных технологий. Представленная в лабораториях совокупность технического оборудования позволяет в полном объеме сформировать навыки технического специалиста для выполнения трудовых функций в сфере защиты информации.

Вместе с тем для модернизации деятельности базовых организаций необходим постоянный поиск современных форм взаимодействия и достижения целей их создания. В широком смысле статус базовой организации государств – участников СНГ в сфере образования предполагает создание скоординированного образовательного пространства, обеспечивающего унификацию стандартов, обмен передовым опытом и интеграцию педагогических технологий. Цифровое сопровождение образовательного процесса может выступить ключевым инструментом реализации данной миссии, обеспечивая трансграничное взаимодействие и повышение качества образования и научных исследований за счет внедрения инновационных технологий.

Цифровое сопровождение образовательного процесса представляет собой системное применение цифровых технологий для управления, организации и контроля образовательной деятельности. В контексте базовой организации СНГ его реализация должна базироваться на принципах интеграции образовательных систем и межкультурной коммуникации.

Это предполагает создание единой цифровой платформы, объединяющей учебные заведения стран-участниц для обеспечения доступа к образовательным ресурсам и программам. Большое значение имеет развитие цифровых инструментов для академического сотрудничества, включая виртуальные академические обмены и совместные исследовательские проекты.

Авторы уже освещали актуальные направления развития межгосударственной системы подготовки профессиональных кадров на основе анализа деятельности базовых организаций и курирующих их органов отраслевого сотрудничества СНГ. Заслуживает внимания предложение по формированию электронного информационного ресурса данной системы подготовки кадров, которая будет доступна для специалистов государств – участников Содружества Независимых Государств [9]. Авторы предлагают разместить данный информационный ресурс на интернет-портале СНГ.

По нашему мнению, разработка единой Межгосударственной Образовательной Платформы позволила бы унифицировать доступ к учебным курсам, электронным библиотекам и системам аттестации.

Таким образом, реализация статуса базовой организации государств – участников СНГ с использованием цифрового сопровождения образовательного процесса будет способствовать формированию единого образовательного пространства, основанного на принципах инновационности и академической интеграции. Ключевыми условиями успеха в этом направлении являются разработка межгосударственных цифровых решений, подготовка педагогических и научных кадров. Это позволит не только укрепить сотрудничество между странами СНГ, но и повысить глобальную конкурентоспособность их образовательных систем.

Список литературы

1. Васильев Э. А., Прокофьева Т. В. О противодействии киберпреступности на территории государств – участников Содружества Независимых Государств // Актуальные проблемы сравнительного правоведения и юридической лингвистики : Материалы Шестой международной научно-практической конференции, Москва, 15–16 декабря 2022 года. М. : Московский государственный лингвистический университет, 2024. С. 113–121.
2. Гребнева А. С., Гребнев Д. Ю., Смирнов В. Г. Состояние и тенденции преступности на территории государств – участников Содружества Независимых государств в 2023 году // Право и управление. XXI век. 2024. Т. 20. № 3 (72). С. 27–56.
3. Информация о работе базовых организаций государств – участников Содружества Независимых Государств // ИНТЕРНЕТ-ПОРТАЛ СНГ : [сайт]. URL: <https://e-cis.info/page/3654/117598/>.
4. Коробейникова О. В. Международное сотрудничество как фактор развития образовательной среды университета // Развитие академических связей в области образования и науки : Материалы двенадцатой международной научно-практической конференции, Братск, 17 декабря 2021 года. Иркутск : Байкальский государственный университет, 2022. С. 46–50.
5. Маруев А. Ю. О базовой организации государств – участников СНГ по исследованию проблем противодействия терроризму и иным проявлениям экстремизма // Международное сотрудничество евразийских государств: политика, экономика, право. 2021. № 4. С. 34–42.
6. Мостович Н. В. Сотрудничество государств – участников СНГ в борьбе с фальшивомонетничеством // Законность и правопорядок в современном обществе. 2011. № 6. С. 193–197.
7. Содружество Независимых Государств: военное сотрудничество и безопасность в XXI веке / [Ю. А. Дашкин, В. А. Чумаков, О. А. Пивень и др.]. М. : Военная академия Генерального штаба Вооруженных Сил Российской Федерации, 2024.
8. Тотоев Р. Р. Проблемы развития международного сотрудничества государств – участников Содружества Независимых Государств в борьбе с незаконным оборотом наркотических средств // На страже закона. 2023. № 3 (3). С. 21–27.
9. Чуйкова Н. А., Гоннова С. М., Разуваева Е. Ю. Межгосударственная система подготовки, профессиональной переподготовки и повышения квалификации кадров для СНГ в новом формате // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2022. № 6. С. 19–28.
10. Jafarov S. Education Policy of 3rd Generation Universities // Revista de Gestao Social e Ambiental. 2024. Vol. 18, No. 6.

Константинов А. В.¹,
заместитель начальника кафедры
противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

OSINT КАК ОБЪЕКТ УГОЛОВНО-ПРАВОВОГО ИССЛЕДОВАНИЯ

Цифровая эпоха, характеризующаяся экспоненциальным ростом объемов информации и повсеместным проникновением информационно-телекоммуникационных технологий в сферы общественной жизни, бизнеса и государственного управления, породила феномен, получивший наименование Open Source Intelligence (OSINT) – разведка на основе открытых источников. Изначально развивавшийся в структурах национальной безопасности и спецслужб, OSINT стремительно трансформировался в универсальный инструментарий, активно используемый в журналистских расследованиях, конкурентной разведке, анализе рисков, проверке контрагентов, поиске активов, управлении репутацией и даже в правоохранительной деятельности.

Сущность OSINT заключается в сборе, обработке и анализе информации, полученной исключительно из общедоступных источников, с целью извлечения полезных, скрытых или неочевидных знаний. Ключевым аспектом является именно «общедоступность» источников, что, на первый взгляд, выводит данную деятельность за рамки правового регулирования, основанного на принципах защиты конфиденциальности и ограничения доступа к закрытой информации.

Вместе с тем стремительное развитие инструментария OSINT, появление автоматизированных систем сбора и анализа данных, а также рост сложности и изощренности методов «цифрового следа» ставят перед правовой наукой и правоприменительной практикой ряд фундаментальных вопросов. Особую остроту эти вопросы приобретают в контексте уголовного права, поскольку деятельность, формально основанная на работе с открытыми данными, может:

1. Выступать в качестве «метода» или «инструмента» совершения уголовно наказуемого деяния.
2. Сама по себе, при определенных условиях и в зависимости от «способа» сбора или «цели» использования данных, потенциально содержать признаки состава преступления.

Таким образом, OSINT перестает быть исключительно технической или оперативной дисциплиной и становится объектом пристального уголовно-правового исследования. Необходимость осмысления правовой природы OSINT, определения границ его легитимности, выявления потенциальных уголовно-правовых рисков и выработки механизмов их минимизации обуславливает актуальность обозначенного вопроса.

¹ © Константинов А. В., 2025.

Разделение между легитимным OSINT и потенциально незаконной деятельностью. Использование взлома, фишинга, социальной инженерии для получения доступа к «непубличной» информации, даже если она впоследствии публикуется, не является OSINT в строгом смысле, а относится к иным видам противоправной деятельности в сфере информационных технологий или против собственности/личности. Определение граней между допустимым сбором и нарушением прав требует развития нормативной базы и экспертного подхода.

В зависимости от объекта исследования и применяемых методов OSINT может классифицироваться по различным признакам, одним из которых является степень автоматизации.

Именно степень автоматизации и масштабы сбора данных, а также последующие действия с собранной информацией (хранение, систематизация, распространение, использование для воздействия), создают основные правовые риски и требуют особого внимания с точки зрения уголовного права.

Также стоит выделить еще одну правовую дилемму OSINT, которая заключается в следующем: если информация является «общедоступной», означает ли это, что ее сбор, хранение, обработка и использование в любых целях, включая те, которые могут нанести вред интересам других лиц или общества, является безусловно правомерным?

Коллизия возникает на уровне интерпретации:

1. Является ли информация, размещенная пользователем в открытом профиле социальной сети, «сделанной общедоступной субъектом» в смысле Федерального закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее также ФЗ-152) [2]? Очевидно, да.

2. Означает ли это, что «любая» обработка этих данных «любим» лицом в «любых» целях правомерна? Нет. ФЗ-152 устанавливает принципы обработки (законность, добросовестность, соответствие целям), требует согласия субъекта на определенные виды обработки и устанавливает ограничения на распространение и использование.

Таким образом, даже работа с общедоступными данными, если они содержат персональные данные, подпадает под действие ФЗ-152. Масштабный сбор (парсинг) открытых профилей, их систематизация, создание баз данных, содержащих персональные данные, без явного согласия субъекта или иного законного основания может быть квалифицировано как незаконная обработка персональных данных.

Гораздо более сложный и дискуссионный вопрос является то, что может ли сама деятельность по сбору, обработке и анализу «открытых» данных при определенных обстоятельствах содержать признаки состава преступления? Прямого запрета на OSINT в УК РФ нет. Однако отдельные действия, совершаемые в рамках OSINT или под его прикрытием, могут подпадать под статьи, криминализирующие деяния в сфере информационных технологий и против конституционных прав граждан. Особое место занимает новая статья УК РФ – ст. 272.1 УК РФ.

В данный момент времени использование инструментов OSINT и соответственно предоставление услуг в сфере OSINT находится в ситуации правовой неопределенности и в состоянии ожидания правоприменительной практики

по ст. 272.1 УК РФ. В связи с этим стоит обозначить современную востребованность, а также актуальность исследования и изучения дисциплины OSINT в контексте юридино-технического понимания.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.
3. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. 2024. № 5. С. 149–155.
4. The use of artificial intelligence and other technologies in criminal proceedings: problems, solutions and prospects / S. Rastoropov, A. Solomatina, V. Yakovleva [et al.] // Relacoes Internacionais no Mundo Atual. 2024. Vol. 3, No. 45. P. 381–391.

Эрдниев А. С.¹,
*начальник учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат педагогических наук*

ОБ ОСОБЕННОСТЯХ ПОДГОТОВКИ ИНОСТРАННЫХ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СОВРЕМЕННОМ ЭТАПЕ

Одной из важнейших задач ведомственной систем является подготовка квалифицированных специалистов для правоохранительных органов стран-партнеров Российской Федерации. Подготовка данной категории слушателей обладает определенной спецификой и, зачастую, значительно отличается от сценариев организации образовательного процесса, применяемых в отношении отечественных обучающихся. В статье предлагается рассмотреть опыт подготовки иностранных слушателей на базе Московского университета МВД России имени В.Я. Кикотя (далее – Университет) по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере (далее – БИТ в ПД).

Отдельный вопрос вызывает выбор специализации в рамках искомой специальности. Ключевым ориентиром для понимания ожидаемого результата выступают квалификационные требования к выпускнику, освоившему ту или иную специальность. В рамках существующей образовательной парадигмы по специальности БИТ в ПД организуется подготовка кадров по таким направлениям, как: компьютерная экспертиза, оперативно-техническое обеспечение расследования и раскрытия преступлений в сфере компьютерной информации, информационно-аналитического обеспечения правоохранительной деятельности и технологии защиты информации в правоохранительной сфере.

Квалификационные требования к выпускнику основываются на ключевых трудовых функция, выполняемых сотрудником в рамках служебной деятельности. В свою очередь в основе данных трудовых функций лежат нормативные акты, определяющие и содержание. Учитывая, что на современном этапе оперативно-техническое обеспечение и информационно-аналитическая составляющая предполагает изучение ведомственных приказов, содержащих сведения, составляющие государственную тайну, возможность обучения иностранных специалистов по данному направлениям подготовки исключается. Компьютерная экспертиза предполагает получение самостоятельного допуска для проведения отдельного вида экспертиз, в соответствии с законодательство Российской Федерации, подобное направление исключено из обучения для иностранных специалистов. Вместе с тем ограничения, связанные с выбором специализации не влияют на сущность образовательной подготовки в рамках специальности БИТ в ПД,

¹ © Эрдниев А. С., 2025.

итоговый результат по всем направлениям подготовки – это получение диплома специалиста в сфере защиты информации.

Образовательный процесс осуществляется, учитывая специализацию «Технология защиты информации в правоохранительной сфере». Подготовка технических специалистов формирует три уровня компетенций: базовые технические знания, умения в сфере защиты информации, обеспечение защиты ведомственных информационных систем.

Но до перехода к образовательной подготовке, основанной на компетентностной модели, подготовка иностранных специалистов связывается с социокультурной адаптацией: изучением русского языка, культурных традиций, философско-этических категорий правоохранительной деятельности и т. д.

Условный предварительный этап обучения во многом зависит от понимания уровня подготовки иностранного специалиста. В исследовании [1] анализируется проблема разного качества базовых знаний, которыми обладают слушатели. Решение проблемы видится в индивидуальной образовательной траектории под каждого обучающегося на основе личностно-ориентированного, прагматического и тезаурусного подходов. Предложение ученых не безосновательно. Однако идеальная реализация под каждого обучающегося в полной мере не реализуема. Вместе с тем, педагогическим коллективом проводится первоначальная диагностика уровня подготовки обучающихся, по результатам которой образовательная модель корректируется и учитываются интеллектуальные особенности слушателей на этапе первоначального погружения в образовательный процесс.

Отдельного внимания заслуживает изучение русского языка как иностранного. В трудах ученых [2, с. 12] рассматривается проблема учета коммуникативных потребностей в социально-бытовой и научной сферах в период обучения в высшей школе. Схожие задачи решает и коллектив Университета. Обучение русскому языку – это не только решение проблемы коммуникации, но и создание позитивной мотивации к обучению.

После преодоления подготовительного этапа, образовательный процесс направляет ориентацию в сторону компетентностной модели. Первый набор компетенций связан с пониманием физических процессов, погружением в знания методов математической обработки данных, к ним относятся:

- использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач;
- применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач;
- применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач.

На данном этапе существуют свои проблемы в подготовке кадров. Несмотря на универсальность математического аппарата, уровень представлений о математическом моделировании у каждого представителя иностранных государств

различен. В исследовании [3, с. 210] обращено внимание на применение отдельных педагогических методов для повышения качества подготовки, таких как разработки тезаурусов на двух языках, использование опорных конспектов при проведении лекционных занятий, с разъяснением математического аппарата, исключении специфических математических оборотов при дискуссии на предметную область и т. д. В полной мере подобные приемы и способы представлены и в рамках образовательного процесса Университета.

Второй набор компетенций предполагает формирование знаний в вопросах применения организационных, криптографических и технических средств обеспечения защиты информации:

- выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации;
- планировать проведение работ по комплексной защите информации на объекте информатизации;
- реализовывать комплекс мер по обеспечению безопасности информации на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;
- применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности;
- осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач;
- использовать автоматизированные информационные системы в профессиональной деятельности;
- понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Данный этап образовательной подготовки наиболее сложен с точки зрения методологического осмысления. Априори педагогическое сообщество полагает, что при формировании устойчивых навыков владения языку государства-обучения и усвоение математического аппарата – достаточное количество факторов, способствующих качественному решению задач на втором этапе обучения. Однако универсальность языка программирования и наличие международных стандартов в сфере защиты информации не решает проблему адаптивности каждого обучающегося. В связи с вышеизложенным в настоящий момент данный этап обучения требует большего научного осмысления нежели все этапы образовательной подготовки.

Третий набор компетенций ориентируется на выполнение конкретных трудовых функций:

- выполнять задачи по проектированию системы защиты информации объектов информатизации и информационных систем;
- разрабатывать проекты нормативно-методических и организационно-распорядительных документов, регламентирующих работу по защите информации;
- разрабатывать модели угроз информационной безопасности систем и сетей;

- проводить работы по установке, настройке, техническому обслуживанию, мониторингу работоспособности аппаратных, программных, программно-аппаратных средств защиты информации (в том числе на основе методов криптографического преобразования), а также средств и систем обработки информации в защищенном исполнении;

- принимать участие в обследовании объектов защиты, их аттестации, контроле защищенности информации;

- проводить мероприятия по защите информации при эксплуатации аттестованных объектов информатизации и информационных систем.

Завершающий этап образовательного процесса наиболее сложен с точки зрения адаптивности к системам защиты информации иностранных государств. Отечественная правовая природа информационной безопасности позволяет получить сведения в свободном доступе о всех нормативных основаниях организации процесса обеспечения защиты информации. Однако процесс выполнения отдельных трудовых функций, связывается с применением специальных методик и исследований, ограниченных в изучении соответствующим правовым режимом.

В иностранных государствах вопросы обеспечения безопасности информации, с точки зрения правовой регламентации различны. Некоторые государства ориентируются на международные стандарты в сфере защиты информации и этим ограничивают нормативную регламентацию информационной безопасности. Отдельные государственные образования разрабатывают целые национальные правовые системы, при этом вводят для них специальный правовой режим, исключающий возможность изучения опыта правового обеспечения информационной безопасности в стране.

Адаптация конкретных дисциплин, направленных на формирование специальных профессиональных компетенций – задача творческая, зачастую трудно реализуемая. Возможный сценарий преодоления препятствий в ориентации образовательного процесса под потребности заказчика заключается в использовании платформы международных соглашений.

Важным элементом в осуществлении образовательной деятельности является материально-техническое обеспечение образовательного процесса. Формирование указанного набора компетенций осуществляется на специализированной материально-технической базе учебно-научного комплекса информационных технологий. К ключевым лабораториям и полигонам относятся:

- лаборатория электротехники, электро-, радиоизмерений;
- лаборатория физики (исследования физических процессов);
- лаборатория программно-аппаратных средств обеспечения информационной безопасности;
- лаборатория проектирования систем информационной безопасности.

В лаборатории № 1 осуществляется обучение в рамках таких дисциплин, как: «Основы микропроцессорной техники», «Основы электротехники и радиоэлектроники», «Основы электро-, и радиоизмерений», «Основы электротехники и электроизмерений».

В лаборатории № 2 оборудование предназначено для проведения практических занятий и лабораторных работ по учебным дисциплинам: «Физика», «Физические основы образования технических каналов утечки информации».

Лаборатория № 3 представлена в виде 24 автоматизированных рабочих мест, объединенных локальной вычислительной сетью. Программное обеспечение осваивается в рамках таких дисциплин, как: «Программно-аппаратная защита информации», «Компьютерная разведка», «Аудит безопасности информационных систем», «Защита информации от методов социальной инженерии», «Интеллектуальная обработка данных», «Криптографическая защита информации»

Лаборатория № 4 представлена в виде 24 автоматизированных рабочих мест, с предоставлением доступа к сети Internet. Основной функционал лаборатории связан с проведением практических занятий по дисциплинам: «Основы информационных технологий и кибербезопасности компетентных органов»; «Программирование: языки, методы и технологии»; «Средства вычислительной техники»; «Мультимедийные технологии»; «Базы данных»; «Системы и сети передачи информации»; «Информационные технологии в аналитической разведке»; «Специальные информационные технологии в правоохранительной деятельности».

В настоящий момент ведутся работы по насыщению материально-техническим оборудованием Лаборатории № 5 «Полигон технической защиты информации». Техническое оборудование осваивается в рамках таких дисциплин, как: «Техническая защита информации», «Организационная защита информации», «Программно-аппаратная защита информации», «Физические основы защиты информации».

Комплекс организационных и материально-технических средств обеспечивает подготовку иностранных специалистов в сфере освоения трудовых функций по защите информации в полном объеме. Однако всегда существуют возможности по совершенствованию образовательного процесса.

Подготовка специалистов по специализации «Технологии защиты информации в правоохранительной сфере» – это лишь один из сценариев обеспечения информационной безопасности. Актуальным направлением развития является подготовка кадров в сфере борьбы с киберпреступностью. В этом ключе доступно переработать и адаптировать под иностранных заказчиков образовательную программу по специализации «Информационно-аналитическое обеспечение правоохранительной деятельности», включив в образовательный процесс технологии освоения: предиктивной аналитики, работы с большим массивом данных, искусственных нейронных сетей и машинного обучения, и других инструментариев автоматизированной обработки информации.

Немаловажным компонентом в сфере борьбы с киберпреступлениям является разработка специализированных образовательных программ по подготовке сотрудников для органов предварительного расследования, ориентируя подготовку кадров на процессуальное сопровождение расследования киберпреступлений.

Таким образом, подготовка иностранных специалистов под различные профессиональные задачи – это комплексная работа, требующая постоянного внимания и адаптацию под реалии не только сегодняшнего дня, но и обозримого будущего.

Список литературы

1. Курдубова В. В. Проектирование технологии подготовки иностранных специалистов в образовательных организациях высшего образования российской федерации / В. В. Курдубова, Л. Ю. Монахова // Современные проблемы науки и образования. 2022. № 5.
2. Биченок Л. П. Актуальные технологии преподавания русского языка иностранным военным специалистам на начальном этапе обучения: грамматический курс / Л. П. Биченок // Русский язык в военном вузе. 2024. № 2 (14). С. 12–25.
3. Трансформация технологий и форм обучения математике иностранных студентов / Н. П. Балабаева, Е. А. Барова, Е. А. Энбом и др. // Самарский научный вестник. 2023. Т. 12, № 2. С. 208–214.

*Михайленко Н. В.¹,
доцент кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

КЛЮЧИ ОТ РАЗУМА: СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ

В современном цифровом мире, где информация стала ценнейшим ресурсом, а взаимодействие между людьми все чаще осуществляется через посредничество технологий, особую остроту приобретает проблема социальной инженерии. Этот феномен, основанный на манипулировании человеческим доверием и слабостями, представляет собой серьезную угрозу как для отдельных лиц, так и для организаций, поскольку позволяет злоумышленникам получать доступ к конфиденциальным данным, совершать финансовые махинации и наносить репутационный ущерб. Социальная инженерия, по сути, является «ключом от разума», позволяющим обходить сложные технические барьеры и проникать в самые защищенные системы. В связи с этим назрела необходимость в комплексном правовом анализе этого явления и разработке эффективных мер по противодействию социальной инженерии.

Общепринятого определения термина «кибермошенничество» не существует, но в широком смысле кибермошенничество – это мошенничество, совершенное с применением IT-технологий, или, возвращаясь к традиционному понятию мошенничества, представленному ранее, его можно определить как хищение имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием с использованием IT-технологий.

Поменялась и сама форма потребления, при этом сферы человеческой деятельности изменились практически на всех уровнях. Например, появились сервисы заказа такси с мобильных устройств с множеством дополнительных опций, электронные маркетплейсы, собравшие в одном месте тысячи поставщиков товаров, телемедицина и многое другое.

При этом в мире, в том числе в России, наблюдается ряд глобальных трендов, кардинально меняющих традиционные подходы к предоставлению услуг:

- удобные сервисы (банковские, доставки, телемедицина);
- развитие экосистем на основе технологических компаний и финансовых организаций;
- развитие концепции открытого банкинга (Open banking);
- цифровая экономика;
- ужесточение регулирования криптовалют и развитие цифровых валют центральных банков;

¹ © Михайленко Н. В., 2025.

- рост значимости рисков и вопросов в области кибербезопасности;
- применение искусственного интеллекта.

Таким образом, благодаря цифровизации происходит серьезная трансформация всего общества. Цифровизация экономики стала не только настоящей технической революцией для ее участников, но в то же время источником новых вызовов и угроз. Ведь цифровые технологии – это не только удобные услуги для клиентов, но и «эффективные» инструменты в руках злоумышленников, пользующихся такими преимуществами цифрового мира, как анонимность, трансграничность и скорость совершения операций.

Половина киберпреступлений совершается с использованием сети Интернет, а более трети – с использованием средств мобильной связи. Методы мошенничества также претерпевают изменения. Так, например, ранее популярный среди мошенников скимминг сегодня более не актуален [1], что связано с внедрением банками средств защиты, усилением ответственности за изготовление, покупку, хранение и реализацию поддельных платежных карт, переходом банков на карты с чипом.

По мнению многих экспертов в области кибербезопасности социальная инженерия – один из основных методов мошенничества в XXI в. Даже самые современные и эффективные способы защиты в ряде случаев оказываются бессильны, когда жертва находится под психологическим влиянием злоумышленника. Рич Могулл, директор по исследованиям Gartner в сфере информационной безопасности и рисков, еще в 2004 г. отмечал, что социальная инженерия – более серьезная проблема, чем хакерство: «Люди по своей природе непредсказуемы и подвержены манипуляции и убеждению. Исследования показывают, что у человека существуют определенные поведенческие тенденции, которые можно эксплуатировать при помощи тонкой манипуляции. Многие наиболее разрушительные проникновения в защищенные системы совершаются и будут совершаться методами социального инжиниринга, а не электронного взлома или хакерства» [2].

С сокращением доли скимминга выросла доля социальной инженерии, применяемой в схемах мошенничества. Если в 2014 году ее доля составляла 14 % от всего объема кибермошенничества, в 2017 г. – 23 %, то к 2024 г. она достигла показателя в 90 %.

Можно выделить три этапа эволюции социальной инженерии. Первый – до 2017 г., когда основным способом коммуникаций с клиентами являлись массово рассылаемые SMS-сообщения. Например, с текстом: «Ваша карта заблокирована, перезвоните в банк» и номером телефона «банка». При звонке на этот номер клиент, после психологической обработки от «службы безопасности», в большинстве случаев оставался без денег. Второй – с 2017 г. до 2020 г., когда SMS-сообщения постепенно стали уступать место телефонным звонкам от «службы безопасности банка» или «полиции». Третий этап – с начала 2020 г. и до настоящего времени – это массовые телефонные звонки через IP-телефонию из мошеннических call-центров [7, с. 42].

Телефонное мошенничество – не единственная киберугроза, однако именно она оставляет позади высокотехнологичные инструменты: хищения через удаленное управление ПК клиента или вирусные заражения мобильных телефонов

и пр. Это объясняется, с одной стороны, простотой организации схемы обмана и доверчивостью граждан, с другой – развитием защищенности банковских продуктов и операционных систем от классических способов кибермошенничества (заражение вредоносным ПО, компрометация данных банковских карт, эксплуатация уязвимостей ПО и пр.).

В настоящее время методы социальной инженерии являются наиболее популярными у мошенников и могут быть реализованы через любые каналы коммуникаций с жертвой (телефония, электронная почта, мессенджеры и пр.). Способы воздействия на жертву с применением методов социальной инженерии с использованием IT-технологий включают: вишинг, фишинг и смишинг, скамминг. Способы воздействия социальной инженерии без использования IT – это мошенничество с использованием фиктивных документов, обман через убеждение и пр. Всего социальная инженерия насчитывает более 170 мошеннических вариаций.

Схемы кибермошенничества с применением методов социальной инженерии относятся к наиболее распространенным: по данным Сбербанка, их общая доля от всех известных схем мошенничества в 2023 г. составила 90 %. Особенностью социальной инженерии является наличие так называемого предлога, с помощью которого мошенник в процессе коммуникации с жертвой вынуждает ее совершить перевод денежных средств на требуемые реквизиты («самоперевод») либо предоставить себе и своим сообщникам банковские данные для доступа к управлению своими счетами («кража личности»).

Для социальной инженерии характерна коммуникация с жертвой через различные каналы связи. В зависимости от канала коммуникации определяется способ реализации социальной инженерии: вишинг (телефонное мошенничество), фишинг (мошенничество с использованием поддельных сайтов и интернет-рассылок), смишинг (SMS-мошенничество) и скамминг (обман при продаже товаров или предоставлении услуг в сети Интернет).

Один и тот же способ мошенничества в социальной инженерии может осуществляться с использованием одного или нескольких каналов коммуникаций с жертвой. Так, например, фишинг может реализовываться через социальные сети, мессенджеры, электронную почту и SMS-сообщения.

На сегодняшний день известно более 100 различных предлогов, их можно выделить в три категории по виду психологического воздействия – чувства страха, жадности и сострадания жертвы.

Во всех случаях мошенники апеллируют к эмоциям своих жертв и требуют от них срочных действий. При запугивании срочность обусловлена серьезными «рисками» («вашему счету угрожает опасность, нужно срочно предпринять действия») в случае «выгодного» предложения – ограниченностью во времени («акция действует только сегодня»), а когда злоумышленники «просят о помощи» – также ограниченностью во времени («нужно срочно совершить перевод»).

Ранее мошенники в большинстве случаев использовали только один предлог в каждой схеме обмана. С 2022 г. они все чаще стали комбинировать различные предлоги в рамках одной схемы.

Вишинг (англ. vishing от voice phishing «голосовой фишинг» или «телефонное мошенничество») – способ кибермошенничества с применением социальной инженерии, реализуемый через телефонные звонки.

Телефонное мошенничество в России появилось в 90-х гг. XX в. и развивалось параллельно с банковскими сервисами и распространением сети Интернет. В отличие от современного вишинга, при котором основной целью является хищение денежных средств со счетов жертв, на заре телефонного мошенничества злоумышленники использовали особенности устройства телефонных сетей для осуществления междугородних звонков за чужой счет. Жертвы мошенников были вынуждены оплачивать официальные счета за звонки, которых они не совершали. Так, например, в «Российской газете» от 15 января 1999 г. опубликована статья «Телефонные пираты начинают и, кажется, выигрывают» [3] с описанием подобных случаев.

На сегодняшний день существует три наиболее распространенных технических решения для совершения мошеннических звонков: IP-телефония, мессенджеры и SIM-box. Использование традиционной телефонии со стационарных телефонов, а также сотовой связи традиционным образом давно не практикуется злоумышленниками по причине введения операторами сотовой связи системы противодействия подмене номера.

Противодействие вишингу со стороны банков технически осуществляется с помощью системы фрод-мониторинга. Его алгоритмы настраиваются в зависимости от схемы мошенничества и учитывают информацию от операторов сотовой связи.

Для выявления подозрительных операций система фрод-мониторинга использует более 1000 различных рискованных признаков: регистрация банковского приложения на новом устройстве, быстрая смена геолокации, нетипичный для клиента перевод, время проведения операции, сомнительный получатель, типичность операции для данного клиента, факт получения кредита непосредственно до перевода, досрочное закрытие вкладов с существенной потерей процентов и пр.

По результатам оценки риска проведение операции может быть приостановлено банком и направлено на дополнительное подтверждение. Клиент информируется о возможном мошенничестве и рекомендуемых действиях. Для разных схем мошенничества используются разные способы подтверждения операций. Операция может быть подтверждена способами, предполагающими контакт с клиентами на исходящем звонке фрод-верификатором, через сотрудника в офисе банка или подтверждение операций автоматизированными способами, например, биометрией в мобильном приложении.

Наиболее часто встречающимися схемами вишинга являются «обман под видом службы безопасности», «привлечение к вымышленному расследованию», а также «обман с использованием QR-кода», «родственник в беде», «удаленное управление устройством под видом технической поддержки», «“Ошибочный” перевод», «фиктивные социальные выплаты и компенсации», «предложение “чудодейственных таблеток”», «замена денежных знаков, “вышедших из оборота”», «обман публичных людей от имени знакомых» и пр.

Социальная инженерия представляет собой многогранный и динамично развивающийся феномен, требующий пристального внимания со стороны законодателя и правоприменителя. Несмотря на то, что отдельные аспекты социальной инженерии, такие как фишинг, мошенничество и неправомерный доступ к компьютерной информации, уже регулируются действующим законодательством, отсутствует комплексный подход к правовому регулированию этого явления.

Анализ существующего законодательства показал наличие ряда пробелов и коллизий, которые затрудняют эффективное противодействие социальной инженерии. В частности, не всегда удается четко квалифицировать действия злоумышленников, использующих методы социальной инженерии, а также установить причинно-следственную связь между этими действиями и причиненным ущербом. Кроме того, существующие правовые нормы не в полной мере учитывают специфику социальной инженерии как метода, основанного на манипулировании человеческим доверием и психологических особенностях.

В связи с этим необходимо совершенствовать правовое регулирование социальной инженерии, в том числе путем внесения изменений в уголовное, гражданское и административное законодательство, которые бы четко определяли понятия и виды социальной инженерии, устанавливали ответственность за совершение соответствующих правонарушений, а также предусматривал меры по профилактике и защите от социальной инженерии.

Эффективное противодействие социальной инженерии требует комплексного подхода, включающего не только совершенствование правового регулирования, но и повышение уровня информационной грамотности граждан, разработку технических средств защиты, а также взаимодействие между правоохранительными органами, бизнесом и обществом. Только совместными усилиями можно создать надежный барьер на пути злоумышленников, использующих «ключи от разума» для достижения своих преступных целей.

Список литературы

1. Сбербанк заявил о победе над скиммерами в России // РБК. URL: <https://www.rbc.ru/finances/19/06/2019/5d0a4c729a79474e473d7dd4>.
2. Gartner: главную угрозу для безопасности представляет социальный инжиниринг // SecurityLab. URL: <https://www.securitylab.ru/news/214555.php>
3. Телефонное мошенничество // КиберЛенинка. URL: <https://cyberleninka.ru/article/n/telefonnoe-moshennichestvo>.
4. Михайленко Н. В. Повышение эффективности управленческого процесса при расследовании преступлений в сфере компьютерной информации или с применением компьютерных технологий // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов, Москва, 30 марта 2023 года / Сост. А. В. Константинов. М. : Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя, 2023. С. 113–116.

5. Гончар В. В., Грибкова К. А., Михайленко Н. В. и др. Организация расследования хищений денежных средств из банкоматов : учебное пособие. Казань : Бук, 2021.
6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. М. : Ай Пи Ар Медиа, 2025.
7. Краснопольский В. В. Проблемы информационной безопасности коммерческого банка в современных условиях / Трансформация глобальной экономики = Global Economy Transformation : сборник научных трудов студентов, магистров и аспирантов / отв. ред. И. А. Айдрус. М. : РУДН, 2022. С. 38–47.
8. Константинов А. В., Михайленко Н. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы // Вестник Московского университета МВД России. 2023. № 3. С. 129–132.
9. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. М. : Ай Пи Ар Медиа, 2025.

Власов П. Е.¹,

*докторант центра организационного
обеспечения научной деятельности
ФГКУ «ВНИИ МВД России»,
кандидат юридических наук, доцент*

НЕКОТОРЫЕ ИЗ ДОПУСТИМЫХ НАПРАВЛЕНИЙ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННЫХ КОГНИТИВНЫХ СИСТЕМ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Происходящее цифровизационное развитие существенно расширило границы использования современных технологий и систем. Некоторые из технологических решений стали доступны для широкого круга пользователей, а современные средства коммуникации в наши дни – неотъемлемая часть жизни общества.

Новейшим направлением цифровизации стало внедрение так называемого «искусственного интеллекта» (ИИ, ИИ-система) – систем и алгоритмов искусственных когнитивных связей, функционирование которых строится на аналогии с нейронами человеческого мозга. Развитие данного направления было сопряжено с появлением технологических решений, позволивших исключить использование существенных вычислительных мощностей – программы или сервисы, использующие алгоритмы ИИ-систем, теперь используют серверные мощности компании, обслуживающей конкретную программу, а для некоторых приложений достаточно вычислительной мощности современного персонального компьютера.

Например, для работы DeepDream, сервисы которого позволяют преобразовывать изображения с учетом пожеланий пользователя, но в соответствии с натренированными весами связей между слоями нейронной сети, на основе которой функционирует система (DeepDream «искажает» (дополняет, изменяет – прим. авт.) исходное изображение в соответствии с тем, какие его фрагменты напоминают алгоритму те или иные знакомые объекты, использованные при его обучении) достаточно компьютера, работающего под управлением одной из операционных систем – Ubuntu Linux, RedHat Linux или OS X, с установленной видеокартой Nvidia, поддерживающей технологию параллельных вычислений CUDA [1; 2, с. 23].

Справедливости ради отметим, что на настоящей момент никакого «искусственного интеллекта» не существует, нет системы, которая бы в полной мере могла имитировать когнитивные функции человека, т. е. самообучаясь «думать» и «принимать решения» без заранее заданного алгоритма. Причем именно «алгоритмизация», лежащая в основе функционирования имеющихся прототипов искусственных когнитивных систем, по нашему мнению, не позволяет говорить о существовании «искусственного интеллекта».

¹ © Власов П. Е., 2025.

Вместе с тем, достигнутый уровень развития ИИ-систем наметил различные тенденции его применения и использования в сфере уголовных и уголовно-процессуальных правоотношений. Однако к технологиям, использующим алгоритмы искусственных когнитивных систем, к допустимости их использования в процессуальной деятельности, правоприменители относятся достаточно консервативно, прежде всего потому, и как отмечают сами разработчики таких систем, что принципы функционирования искусственного интеллекта остаются еще достаточно иллюзорными из-за низкой прозрачности и отслеживаемости причинно-следственных связей в итоговом результате, выдаваемом пользователю [3, с. 149]. Таким системам присуща непрозрачность и предвзятость [4, с. 488–515; 5, с. 157–182; 6, с. 18–21].

Однако было бы неправильно игнорировать и избегать использование имеющихся уже на сегодня технологий ИИ в достижении назначения уголовного судопроизводства.

Так, для моделирования изображений по текстовому запросу, для изменения внешности, голоса человека в реальном времени используются технологии *deepfake* [7]. Данные технологии также используются для совершения преступлений, связанных с неправомерным завладением денежными средствами, находящимися на вкладах и счетах граждан. В случае закрепления в УК РФ в качестве отягчающего наказание обстоятельства применение искусственного интеллекта при совершении преступлений [8], это потребует адаптации процессуального доказывания - в соответствии с п. 6 ч. 1 ст. 73 УПК РФ, в соответствии с которым обязательному установлению подлежат смягчающие и отягчающие наказание обстоятельства.

Вместе с тем, основываясь на познаниях сущности функционирования искусственных когнитивных систем, в обозримой перспективе будет достаточно сложным доказывание использования технологий *deepfake* в качестве обстоятельств, предусмотренных п. 6 ч. 1 ст. 73 УПК РФ.

Затронув тему компьютерного моделирования и исходя из возможностей технологий *deepfake* следующим направлением допустимого использования технологий искусственных когнитивных систем в уголовном судопроизводстве, считаем их использование в судебной экспертной деятельности [3, с. 256, 355 и др.]. Правовым основанием для этого, помимо прочих, могут являться положения ГОСТ Р ИСО/МЭК 30121-2017, в соответствии с которыми предусмотрено проведение судебной экспертизы свидетельств, представленных в цифровой форме.

При производстве судебных экспертиз могут использоваться создаваемые 3D-модели. О перспективности такого направления говорят многие ученые [9, с. 99–106; 10, с. 377–381; 11, с. 234–236; 12].

Использование технологий дополненной, виртуальной и смешанной реальности [13] возможно при производстве ряда следственных действий, где, в определенной степени, необходимо воссоздать обстановку проверяемого события, либо смоделировать ситуацию, направленную на стимулирование воспоминаний. Данные технологии, основанные на алгоритмах «искусственного интеллекта», в случае законодательного закрепления соответствующих положений в УПК РФ, можно было бы использовать при производстве допросов, повторных осмотров

места происшествия, следственного эксперимента и проверки показаний на месте. Ряд авторов уже сейчас предлагает включить использование таких технологий в процессуальную деятельность, например, для обеспечения возможного участия в следственном действии одного из входящих в следственную группу следователей, но находящегося вне места его производства [14, с. 252–253]. Полагаем подобным образом использовать данные технологии в судебных заседаниях, для демонстрации, например, обстановки осмотренного места происшествия, следов, образованных в условиях негативного влияния свойств объектов или действия факторов внешней среды и пр.

Допустимость использования в уголовном судопроизводстве обозначенных в настоящей работе некоторых технологических решений, использующих алгоритмы «искусственного интеллекта», сопряжена с техническим разрешением вопросов, связанных с конфиденциальностью данных, используемых в работе таких систем.

Big Data – данные, без которых невозможно полноценное функционирование «искусственного интеллекта», хранятся на серверах компаний, осуществляющих разработку и обслуживание данных технологий. Для бытового и коммерческого уровней этого более чем достаточно и приемлемо с позиции используемых охранительных средств. Но использование открытых источников для накопления и хранения процессуальной информации, в особенности используемой в досудебных стадиях и относящейся к конфиденциальной, доступ к которой и степень распространения которой охраняются нормами УПК РФ и являются тайной следствия, недопустимо.

Получается, что для того, чтобы использовать в уголовном судопроизводстве технологии искусственных когнитивных систем необходимо на имеющейся базе технического обеспечения системы правоохранительных органов Российской Федерации создавать соответствующую информационно-цифровую среду, позволяющую обеспечить надлежащее функционирование рассматриваемых технологий в условиях надлежащей сохранности используемых данных. Как отмечают некоторые исследователи, в системе МВД России уже сейчас есть защищенные каналы связи, работа которых осуществляется на ведомственных серверах [14, с. 56–61; 16, с. 111–117]. А. Ю. Чурикова, основываясь на приказе Генерального прокурора, справедливо отмечает, что «для обеспечения информационной безопасности и защищенности персональных данных совершенно обоснованным представляется реализация такой задачи цифровой трансформации прокуратуры как «создание и развитие устойчивой, надежной и безопасной информационно-телекоммуникационной инфраструктуры, реализующей в том числе «сквозные» технологии цифровой экономики и использующей существующие и вновь создаваемые российские центры обработки данных, государственную единую облачную платформу, защищенные сети связи и передачи данных, отечественные цифровые платформы работы с данными» [3, с. 224–225.].

В заключение отметим, что в настоящий момент процессы, связанные с внедрением в уголовное судопроизводство современных технологических решений и систем, одним из видов которых является «искусственный интеллект», находятся в начальной стадии формирования концептуальных подходов. Вместе

с тем значимость таких процессов неоспорима. На данном этапе важно не переоценить возможности рассматриваемых систем, нельзя недооценивать масштаб потенциальных негативных последствий от их использования, прежде всего сопряженных с нарушением законных прав участников уголовного судопроизводства и основополагающих процессуальных принципов.

Список литературы

1. Филиппова Т. Аж глаза на лоб. N+1 предлагает читателям собственный сервис DeepDream // URL: <http://nplus1.ru/material/2015/07/13/use>.
2. Власов П. Е. Дискуссионные направления цифровизации уголовного судопроизводства // Российский следователь. 2024. № 9.
3. Чуриквва А. Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование : дис. ... док-ра юрид. наук. Саратов, 2024.
4. Харитонов Ю. С., Савина В. С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // Вестник Пермского университета. Юридические науки. 2021. № 53.
5. Кузнецов А. Г. Туманности нейросетей: «черные ящики» технологий и наглядные уроки непрозрачности алгоритмов // Социология власти. 2020. Т. 32, № 2.
6. Сумин А. А., Химичева О. В. Искусственный интеллект в уголовном процессе государств Азиатско-Тихоокеанского региона : общий обзор // Международное уголовное право и международная юстиция. 2020. № 2.
7. Воронин И. А., Гавра Д. П. Дипфейки: современное понимание, подходы к определению, характеристики, проблемы и перспективы // Российская школа связей с общественностью. 2024. № 33.
8. Юридическая концепция роботизации: монография / Н. В. Антонова, С. Б. Бальхаева, Ж. А. Гаунова и др. ; отв. ред. Ю. А. Тихомиров, С. Б. Нанба. М. : Проспект, 2019.
9. Коньгин Р. А., Шестакова Л. А. Использование компьютерного трехмерного моделирования в уголовном судопроизводстве Российской Федерации // Юридический вестник Самарского университета. 2017. № 3. Т. 3.
10. Кошлыкова Ю. А. Возможности использования 3D-технологий для решения криминалистических задач // Цифровые технологии и право: сб. науч. тр. / [под ред. И. Р. Бегишева и др.]. В 6 т. Т. 4. Казань : Познание, 2022.
11. Овсянников В. В. Перспективы использования 3D-сканирования в экспертной практике // Право и государство: теория и практика. 2020. № 12.
12. Полякова А. В. Формирование и развитие 3D-технологий в судебно-экспертной деятельности: методологические и организационные аспекты : дис. ... канд. юрид. наук. Уфа, 2023.
13. URL: <http://ru.wikipedia.org/>.
14. Смушкин А. Б. Использование компьютерно-опосредованной реальности в правоохранительной деятельности // Вестник Томского государственного университета. 2020. № 454. С. 252–253.

15. Зайцева Е. А. Внедрение дистанционных технологий в отечественном досудебном и судебном производстве по уголовным делам // Проблемы противодействия киберпреступности. М. : Моск. акад. След. ком. РФ, 2023. С. 56–61.

16. Попова О. А. Организационные и процессуальные аспекты участия в уголовном судопроизводстве в режиме удаленного доступа // Вестник Волгоградской академии МВД России. 2020. № 3. С. 111–117.

*Лахтиков Д. Н.¹,
начальник кафедры информационного права
факультета криминальной милиции
Академии Министерства внутренних дел
Республики Беларусь,
кандидат юридических наук, доцент*

НЕЙТРАЛИЗАЦИЯ ФИНАНСОВОЙ СОСТАВЛЯЮЩЕЙ КАК ЭЛЕМЕНТ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Противодействие киберпреступности, являющейся довольно сложным и многогранным явлением, которое представляет угрозу не только в информационной, социально-экономической и других сферах, но и национальной безопасности в целом является задачей, от решения которой во многом зависит безопасность граждан, общества и государства.

В современных условиях одной из тенденций в данной сфере является интенсивное развитие информационных технологий и постоянное совершенствование методики совершения киберпреступлений. Следует отметить, что в свою очередь от преступников требуются определенные финансовые затраты на организацию совершения преступлений либо вывод похищенных средств. В этой связи весьма актуальным при противодействии киберпреступности является деятельность по нейтрализации ее финансовой составляющей, установлению и нейтрализации финансовых потоков.

Преступники противодействуют правоохранительным органам не только на физическом, но и интеллектуальном уровнях, и при осуществлении финансирования своей деятельности максимально используют возможности сокрытия следов, усложнения механизма их установления, с этой целью используют также цифровые финансовые активы (криптовалюты). В современных условиях складывается ситуация, когда воздействие на финансовую составляющую киберпреступности возможно при реализации финансового мониторинга в совокупности с мерами оперативно-розыскного характера.

Развитие сферы цифровых финансовых активов носит глобальный характер, что связано с их технологической и экономической природой – оборот осуществляется трансгранично. Кроме того, многие государства предприняли шаги для регулирования данной сферы, а также для создания в своих юрисдикциях привлекательных условий для осуществления деятельности, связанной с цифровыми финансовыми активами. Внедрение технологии блокчейн в определенной степени ограничило контроль за оборотом последних со стороны правоохранительных органов, что обусловлено преимущественно программно-техническими особенностями.

Отношения в сфере цифровых финансовых активов регулируются Декретом Президента Республики Беларусь № 12 «О Парке высоких технологий» и Декре-

¹ © Лахтиков Д. Н., 2025.

том № 8 «О развитии цифровой экономики»; Указом Президента Республики Беларусь «О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты»; Гражданским кодексом Республики Беларусь; Законом Республики Беларусь «О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения»; постановлением Министерства финансов Республики Беларусь № 16 «О бухгалтерском учете цифровых знаков (токенов)»; актами Наблюдательного совета ПВТ (Положение о требованиях к заявителям, Положение о требованиях к ПВК, Правила деятельности криптоплатформы, Требования к Организатору ICO и др.) Так, Декрет Президента Республики Беларусь № 8 «О развитии цифровой экономики» закрепил такие понятия как виртуальный кошелек, криптовалюта, реестр блоков транзакций (блокчейн), цифровой знак (токен), а также явился определенной правовой базой использования цифровых финансовых активов в Республике Беларусь. В свою очередь, анализ показывает, что имеющаяся правовая база не в полной мере учитывает все возможности противодействия финансовой составляющей преступности.

В Республики Беларусь выстроена система правовых мер, направленная на обнаружение сомнительных финансовых операций, потенциально связанных с легализацией доходов, полученных преступным путем. Она основана на стандартах ФАТФ – межправительственной организации, занимающейся выработкой стандартов в сфере противодействия отмыванию преступных доходов и финансированию терроризма. В соответствии с постановлением Совета Министров Республики Беларусь № 1249 «Об установлении общих требований к правилам внутреннего контроля» юридическими лицами, осуществляющими финансовые операции, самостоятельно определяется порядок контроля над банковскими операциями с учетом общих требований к правилам внутреннего контроля, в том числе определяемых государственными контролирующими органами. Закреплены общие требования к организации внутреннего банковского контроля, при этом банки и иные субъекты имеют право самостоятельно устанавливать идентификаторы риска финансовой операции, а также порядок направления информации о выявлении операций, подлежащих дополнительному контролю в Департамент финансовых расследований Комитета государственного контроля Республики Беларусь. Критерии по отнесению операций к потенциально связанным с предикатными преступлениями у различных субъектов могут отличаться, отдельные из них разрабатываются Национальным Банком Республики Беларусь.

В Беларуси уже сформировалась обширная практика применения имеющегося регулирования, что определяет потребность дальнейшего совершенствования установленных правил уже не в рамках формирования рынка цифровых финансовых активов, а в целях актуализации регулирования с учетом нарабатанной практики, в том числе связанной с предотвращением использования цифровых финансовых активов в преступных целях.

При этом необходимо учитывать, что в силу специфики, присущей цифровым финансовым активам (анонимность, криптографическая защита, отсутствие опе-

ратора и др.), возможности ее применения в преступном мире различны. Изучение международного опыта и научной литературы в рассматриваемой области свидетельствует о том, что в преступных целях цифровые финансовые активы могут использоваться для финансирования экстремизма и терроризма; отмывания и легализации преступных доходов; совершения киберпреступлений; приобретения оружия и вредоносного программного обеспечения; оплаты услуг по осуществлению кибератак и др. [2, с. 137–138].

Отдельные государства закрепили правовые механизмы контроля над цифровыми финансовыми активами и криптобиржи, функционирующие в их правовом поле, не предоставляют возможности проведения транзакций с использованием средств анонимизации, что обусловило появление так называемых криптомиксеров, смешивающих криптовалютные транзакции с транзакциями в целях воспрепятствования анализа для выявления связей между отправителями и получателями, повышая уровень анонимности и конфиденциальности транзакций.

В свою очередь цифровые финансовые активы все чаще используются в оплате товаров или услуг в сети Интернет. Биткоин является наиболее распространенной криптовалютой, которая хранится на криптовалютных адресах в криптовалютных кошельках. Все транзакции, перемещающие криптовалюты с одного адреса на другой, подписаны электронным образом и размещены в биткоин-сети, а также распространяются по всей сети криптовалюты.

Тем не менее использование цифровых финансовых активов не полностью анонимно. Блокчейн не раскрывает никакой информации, которая могла бы привести к идентификации плательщика и получателя. Однако исследование открытого исходного кода, информации, предоставляемой частным сектором, может приводить к идентификации лиц, интересующих правоохранительные органы. В первую очередь представляет интерес информация, имеющаяся у криптобирж. Такой информацией являются контактные данные пользователей, IP-журналы, журналы активности, криптоадреса, используемые пользователем для обмена цифровых финансовых активов, платежные данные и др. Необходимо учитывать, что идентификация возможна на основе криптокошелька, также может реализовываться и транзакционный подход. Преступники используют криптовалюты с повышенным уровнем анонимизации (например, Монеро), возможности криптомиксеров, осуществляют переводы на другие кошельки или иные виды цифровых финансовых активов, при этом изучение международной практики показывает, что возможно установление лиц, совершивших преступление и в таких ситуациях. В процессе осуществления мониторинга финансовых операций все субъекты (банки, криптобиржи и др.) должны выявлять и иметь техническую и правовую возможность блокировать транзакции финансовых средств, отвечающие определенным критериям отнесения операций к потенциально связанным с преступной деятельностью, при этом должен быть налажен оперативный обмен информацией с соответствующими правоохранительными органами. При появлении в поле зрения правоохранительных органов каких-либо лиц, организаций, причастных к рассматриваемой преступной деятельности, мониторинг финансовой активности выступает на передний план, анализируются все финансовые потоки, в том числе с цифровыми финансовыми активами.

В этой связи отдельные авторы отмечают, что эффективным методом мониторинга процесса использования криптовалюты как платежного средства может стать создание на межгосударственном (международном) уровне межведомственных рабочих групп. Целью такой консолидации должна стать выработка средств и методов правового регулирования использования цифровых финансовых активов и создание на этой основе правовой базы для межгосударственного обмена опытом и взаимного оказания правовой помощи и поддержки, направленных на выявление, замораживание, арест и обоснованную конфискацию доходов, полученных от преступлений, связанных с оборотом цифровых финансовых активов [3, с. 75]. Противодействие киберпреступности, реализуемое по данному направлению, требует сотрудничества между правоохранительными органами и финансовыми институтами, в том числе на международном и межгосударственном уровне.

Перспективным представляется совершенствование регулирования деятельности субъектов, участвующих в обороте цифровых финансовых активов, например, в части выработки норм, позволяющих использовать цифровые финансовые активы, изъятые компетентными органами (например, государств-участников соглашения), находящимися в распоряжении криптобиржи, для совершения транзакций с криптобиржами государств-участников соглашения без «понижения рейтинга» криптобиржи.

Касаясь выявления, ареста и конфискации цифровых финансовых активов как в правовом, так и в организационном и техническом планах, также существуют аспекты для улучшения (так, например, возможно совершенствование межгосударственной правовой базы и механизма оперативного блокирования транзакций по обороту цифровых финансовых активов; совершенствование подходов при определении идентификаторов сомнительных транзакций).

Перспективным представляется взаимодействие по совершенствованию и внедрению новых технологий противодействия анонимизации субъектов киберпреступности. Особенно актуальна для правоохранительных органов потребность своевременного обмена не только статистическими данными, но и в первую очередь достоверной информацией, касающейся сомнительных трансграничных операций с использованием цифровых финансовых активов.

Таким образом, потенциальные угрозы, обусловливаемые киберпреступностью, определяют одно из приоритетных направлений в противодействии этому явлению – нейтрализацию финансовой составляющей. Имеющаяся правовая база не в полной мере учитывает все возможности противодействия финансовой составляющей преступности. Необходимо нейтрализовывать организационную и технологическую инфраструктуру противоборствующей стороны, обеспечивать привлечение к уголовной ответственности не только организаторов, но и исполнителей любого уровня.

Рост использования цифровых финансовых активов в преступной деятельности связан с особенностями используемой технологии, для которой характерны децентрализация эмиссии и оборота, отсутствие эффективного регулирования, определенная степень анонимности. Базовым принципом блокчейна являются прозрачность и публичность транзакций, что позволяет в определенной степени

отследить цепочку операций участника сети, определить периодичность и объем переводов; установить адреса, с которых переводили суммы и другую значимую информацию.

Список литературы

1. Авхадеева Л. Ш. Криптовалюта и преступность // Вестн. Барнаульск. ин-та МВД России. 2019. № 2 (37). С. 137–139.
2. Авхадеева Л. Ш. К проблеме инструментов противодействия преступлениям, совершаемым с использованием криптовалют: гражданско-правовой и уголовно-правовой аспекты // Вестн. Калининградского филиала Санкт-Петербургского ун-та МВД России. 2020. № 4 (62). С. 71–76.

РАЗДЕЛ II. ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

*Апаев И. Х.¹,
старший преподаватель кафедры
оперативно-разыскной деятельности
и специальной техники
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук*

*Солодар Д. Д.²,
курсант факультета подготовки сотрудников
для оперативных подразделений полиции
Московского университета
МВД России имени В.Я. Кикотя*

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В последние десятилетия мир столкнулся с резким ростом развития технологий и глобализацией, в связи с чем происходит модификация способов совершения преступлений, а также происходит изменение личности преступника. Борьба с новыми видами преступлений традиционными методами становится все менее эффективной. В этом контексте внимание правоохранительных органов привлекает искусственный интеллект, как наиболее перспективный инструмент для выявления, предупреждения, пресечения и раскрытия преступлений.

Примеры использования ИИ иностранными государствами в целях предупреждения и пресечения преступлений демонстрируют положительные результаты в данном направлении. Успешный опыт других стран в использовании искусственного интеллекта в рамках деятельности по предупреждению преступлений демонстрирует целесообразность внедрения аналогичных программ в российских реалиях. Внедренные программы на базе искусственного интеллекта в работе органов других стран представлены в *табл. 1*.

Целью и задачами исследования являются изучение и выявление теоретических основ и практических аспектов использования искусственного интеллекта в деятельности оперативных подразделений ОВД.

¹ © Апаев И. Х., 2025.

² © Солодар Д. Д., 2025.

В качестве методов исследования использовались сравнительный анализ внедрения ИИ в зарубежных странах, оценка влияния ИИ на эффективность деятельности правоохранительных органов.

Внедрение ИИ в органы внутренних дел обуславливает накопление большого массива данных в интернет-пространстве. Становятся необходимы структуризация информации и выдача наиболее подходящего ответа на поисковой запрос. Сервисы ИИ с высокой скоростью анализируют все интернет-источники и выдают оптимальный результат для пользователя. Более того, при функционировании данной технологии человеческий фактор нивелируется, поскольку искусственный интеллект отличается самостоятельностью в процессах сбора и обработки сведений, тем самым выдавая наиболее точный и подходящий по запросу ответ.

Таблица 1

Искусственный интеллект в предупреждении преступности¹

Наименование программы (эксперимента) / Name of the program (experiment)	Сфера применения / Sphere of use
Интегрированная геолокационная платформа предиктивной аналитики (Манчестер, Великобритания, 2016 г. – н. в.)	Профилактика уличной преступности за счет повышенного внимания полиции к улице или участнику улицы при изменении факторов, воздействующих на уровень данного вида преступности
Система анализа данных, основанная на разработках IBM и географической информационной системе Ersi (Ванкувер, Канада, 2007 г. – по н. в.)	Выявление тенденций преступности, прогнозирование вероятного времени и места совершения. С 2007 по 2011 гг. количество преступлений, связанных с собственностью, сократилось на 24 % уровень насильственной преступности – на 9 %
Эксперимент, направленный на профилактику индивидуальной преступности рецидивистов (Квебек, Канада, 2015 г. – по н. в.)	Находящимся в заключении рецидивистам с учетом тяжести их преступлений предлагается условно-досрочное освобождение в обмен на согласие разместить на своем теле татуировку, представляющую собой сверхтонкий процессор-индикатор, который меняется раз в пять лет
Программа по созданию системы социального кредита (КНР, 2014–2020 гг.)	К 2020 г. планируется отслеживать и оценивать в режиме реального времени каждого жителя материкового Китая. Рейтинг доверия физических лиц привязывается к социальному паспорту. Обладатели высокого рейтинга пользуются различными социальными и экономическими льготами, обладатели низкого рейтинга попадают под административные санкции и ограничения

Интеграция системы искусственного интеллекта для ведения той или иной деятельности заключается в потребности автоматизации рутинных задач, с которыми ранее сталкивался человек. Искусственному интеллекту не свойственны

¹ Составлено автором на основании научной статьи А. П. Суходолова и А. М. Бычковой [5].

погрешности и опечатки, которые имеют место при выполнении монотонных задач человеком. Внедрение данной технологии позволяет сконцентрировать человеческий потенциал на более масштабных и глобальных направлениях вместо однотипной работы.

Использование технологий ИИ в деятельность оперативных подразделений по пресечению и раскрытию преступных деяний играет ключевую роль, как и в ходе предупреждения и выявления преступлений, дает возможность скоростной обработки больших объемов данных. В настоящее время достаточно результативной системой в городе Москва является аппаратно-программный комплекс «Безопасный город» (далее – АПК «БГ»), регламентируемый Постановлением Правительства г. Москвы от 23.09.2011 № 443-ПП, в соответствии с которым выделяется цель «повышения эффективности обеспечения безопасности граждан и защиты объектов жизнеобеспечения города Москвы», который активно внедряется и в другие наиболее крупные города России, такие как Санкт-Петербург, Казань и Екатеринбург.

АПК «Безопасный город» основан на сервисах ИИ, что предусматривает широкий круг возможностей при применении его в деятельности оперативных подразделений ОВД. Он включает в себя множество различных модулей. Основными для деятельности оперативных подразделений ОВД являются модули видеомониторинга и видеоаналитики, взаимодействующие с камерами видеонаблюдения, установленными по всему городу.

Камеры фиксируют все происходящее в городе, что позволяет сотрудникам в онлайн-режиме наблюдать за интересующим объектом. Кроме того, все что записали камеры, сохраняется на сервер ГИС ЕЦХД (Единый центр хранения и обработки данных Москвы), откуда в течение 21 суток (в некоторых случаях 7 суток) можно получить нужный фрагмент происшествия, необходимый для оценки характера преступления, выявления лиц, причастных к совершению преступного деяния, осуществления их поиска и формирования доказательственной базы.

Система обладает функцией распознавания лиц и отслеживания передвижений, а именно в АПК «БГ» интегрирована подсистема автоматической регистрации сценариев индексирования видеoinформации (далее – ПАРСИВ), основанная на ИИ. ПАРСИВ анализирует видеоматериалы, поступающие в ГИС ЕЦХД и сопоставляет их с имеющимися в базе фотографиями фигурантов, после чего выдает отчет, где указаны время, место и фото с камеры. Данный модуль позволяет сотрудникам оперативных подразделений ОВД подключиться к нему в реальном времени с помощью мобильного приложения и получать информацию о местонахождении интересующего следствие лица для оперативного реагирования.

Указанная система успешно функционирует уже четырнадцать лет, что подтверждается и статическими данными, изложенными в Постановлении Правительства г. Москвы от 26 марта 2024 г. № 614-ПП, поскольку посредством действующей умной системы видеонаблюдения и других технологий в рамках АПК «Безопасный город» общая масса преступлений в период с 2010 по 2023 гг. снизилась более чем на 28 % [1].

Полагается, что такая благоприятная динамика связана с наличием у субъекта, который готовится к совершению преступления, информации о действующей системе видеонаблюдения и распознавания лиц, что снижает уровень преступности из-за осознания населением высокого риска привлечения к ответственности.

Следовательно, умная система видеонаблюдения в значительной степени облегчает для оперативных подразделений раскрытие преступлений, так как предоставляет возможность достаточно быстро получать доступ к видеозаписям с камер и анализировать их, в том числе с помощью технологий искусственного интеллекта.

Важным условием в поиске информации оперативными сотрудниками в эпоху цифровизации является то, что большую часть личных данных человека можно найти в открытых источниках. Почти каждый житель нашей планеты имеет хотя бы один аккаунт в социальных сетях и охотно делится своей жизнью на всеобщее обозрение. Фотографии, видеоматериалы, отметки геолокации, комментарии и публикации различных файлов – это детали, с помощью которых можно узнать о человеке многое, в некоторых случаях – все.

Для осуществления поиска человека, его связей, личных данных и местоположения в настоящее время не обязательно использовать скрытые источники информации и сервисы МВД России. Достаточно лишь воспользоваться технологиями OSINT (open source intelligence)-разведка на основе открытых источников [2]. Она открывает перед сотрудниками широкий круг возможностей на этапах, когда использование закрытых источников информации невозможно. Позволяет собирать информацию об интересующих объектах в сети Интернет и анализировать ее.

В связи с накоплением в социальных сетях большого количества данных о пользователях, в OSINT стали внедрять ИИ, который помогает быстрее и качественнее отбирать сведения и предоставлять готовый отчет клиенту. Приведем несколько примеров технологий OSINT, созданных на основе ИИ:

3D Social Graph-приложение в социальной сети «ВКонтакте», создающее социальный граф пользователя, в котором на основе данных о друзьях человека моделируется группы связанных лиц. Чем больше нитей у аккаунта, тем больше он близок интересующему объекту оперативным подразделениям ОВД. Для сотрудников это имеет весомое значение, так как 3D Social Graph помогает нам за считанные секунды получить социальный круг взаимодействия фигуранта.

Глаз бога-телеграм-бот, который аккумулирует в себе данные о различных объектах и лицах, находящихся в общем доступе. Для обычных пользователей мессенджера «Telegram» он является платным, в то время как для оперативных сотрудников ОВД России услуга предоставляется бесплатно, на основе контракта, заключенного с МВД России. С помощью него возможно осуществить поиск по фото, ФИО, номеру телефона, номеру транспортного средства, по ссылке социальной сети и прочее. Имея только маленькую часть пазла, можно собрать полную картину об объекте.

СайтСпутник-приложение, осуществляющее поиск и анализ информации в сети Интернет для составления статистических данных и выявления потенциальных угроз для населения. Для предупреждения и пресечения преступлений эта система является необходимой, так как позволяет за короткий промежуток времени по заданному поисковому вопросу и глубине поиска выявить опасные публикации и пользователей, вовлеченных в противоправную деятельность. Это ускоряет процесс служебной деятельности оперативных сотрудников и позволяет не допускать совершения преступлений.

Возможности открытой разведки OSINT поражают своей доступностью. Это обусловлено тем, что они позволяют органам внутренних дел экономить свои ресурсы, получая максимально объективную и полезную информацию для принятия решений.

OSINT дает возможность применения в служебных и личных целях, что не всегда является положительным аспектом, так как население может использовать знания в преступных целях. Несмотря на свою мощь и полезность, OSINT также вносит свои вызовы и риски. Неправильное использование открытых источников может привести к нарушению законов о конфиденциальности, утечке информации и нарушению частной жизни.

Искусственный интеллект представляет собой перспективную технологию, активно применяющуюся в различных сферах общественной жизни. В условиях цифровизации внедрение искусственного интеллекта в правовое пространство становится особенно актуальным, повышая эффективность и прозрачность уголовного судопроизводства.

Анализ направлений использования искусственного интеллекта в деятельности органов внутренних дел продемонстрировал, что указанная технология может быть эффективно применена для автоматизации процессов идентификации и анализа данных о лицах и транспортных средствах, контроля доступа на охраняемые территории, проверки подлинности документов и выявления признаков серийных преступлений.

Подводя итог всему вышеизложенному, хотелось бы отметить, что внедрение искусственного интеллекта в деятельность оперативных подразделений является перспективным направлением, которое может существенно повысить эффективность работы органов. Однако для успешного внедрения этой технологии необходимо учитывать риски и проблемы, связанные с ее использованием, и сформировать соответствующие меры по их управлению.

Список литературы

1. О внесении изменений в постановление Правительства г. Москвы от 23 сентября 2011 г. № 443-ПП : Постановление Правительства г. Москвы от 26 марта 2024 г. № 614-ПП // Вестник Москвы. Т. 1. № 39. 16 июля.
2. Дворянкин О. А. OSINT, PENTEST и НЕТСТАЛКИНГ – информационные технологии Интернета // Национальная ассоциация ученых (НАУ) № 84, 2022.

3. Елисеев А. В., Агафонов С. И. К вопросу о правоохранительном сегменте АПК «Безопасный город» // Вестник Московского университета МВД России. 2016. № 7 С. 139–142.
4. Кофман Д. В. Использование аппаратно-программного комплекса «Безопасный город» в целях выявления и раскрытия преступлений // Международный научный журнал «Молодой ученый». 2023. № 38 (485). С. 117–119.
5. Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. № 6. С. 753–766.

Баранов А. А.¹,
доцент кафедры криминологии
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

Соломатина Е. А.²,
доцент кафедры криминологии
Московского университета
МВД России имени В.Я. Кикотя,
доцент кафедры уголовно-правовых дисциплин
Международного юридического института,
кандидат юридических наук, доцент

К ВОПРОСУ О МЕРАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫХ ПРОТИВ НЕСОВЕРШЕННОЛЕТНИХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Сегодня в жизни молодых людей информационно-телекоммуникационные технологии занимают важное место, многие уже не представляют жизни без них. Интернет-пространство дает им не только возможность для развития, общения и получения информации, но и является пространством, где они могут столкнуться и с определенными угрозами, опасностями и совершением IT-преступлений в отношении них. Сегодня такие преступления носят достаточно разноплановый характер, начиная от «кибербуллинга», «секстинга», «грумминга» и заканчивая нарушением конфиденциальности личных данных, распространением вредоносного контента и другими [1].

Несовершеннолетние, как правило, обладающие ограниченными знаниями о правилах безопасного нахождения в онлайн-среде, являются соответственно более уязвимой жертвой по сравнению со взрослыми.

Отметим, что в настоящее время разработаны и эффективно работают стратегии защиты детей и подростков в Интернете [2–5]. Однако технологический прогресс не стоит на месте и анализ существующих проблем, связанных с интернет-безопасностью несовершеннолетних видится достаточно актуальным.

Ввиду стремительно развивающихся цифровых угроз существующие на данный момент защиты уже не являются передовыми, которые в полной мере могли бы защитить несовершеннолетних. Более того, значительное число их уже подвергались преступному воздействию, но не говорили об этом родителям. Также следует учитывать, что данные преступления наносят серьезный вред психическому здоровью детей, приводят к эмоциональной травме и более трагическим последствиям.

¹ © Баранов А. А., 2025.

² © Соломатина Е. А., 2025.

Так, по данным Следственного комитета РФ в 2020 г. было расследовано 1169 преступлений в отношении детей с использованием Интернета. По итогам 2021 г. рост таких преступлений составил +84 % (2 150). Подавляющее число несовершеннолетних при этом пострадали от преступлений на сексуальной почве и различных хищений. В 2023 г. и в 2024 г. более 1 тыс. преступлений были сопряжены с посягательством на половую свободу несовершеннолетних в сети Интернет, а 4 тыс. преступлений, были связаны с распространением порнографических материалов в сети с изображением несовершеннолетних.

В связи с чем необходимо обратить внимание на наиболее эффективные меры противодействия преступлениям, совершаемых против несовершеннолетних с применением информационно-телекоммуникационных технологий.

Так, среди правовых мер противодействия преступлениям, совершаемых против несовершеннолетних, выделим совершенствование законодательства, относящееся на наш взгляд к числу наиболее приоритетных. Увеличение сроков лишения свободы и введение дополнительных квалифицирующих признаков для ряда статей уголовного законодательства, за совершение преступлений против несовершеннолетних с применением информационно-телекоммуникационных технологий, по нашему мнению, дало бы положительный эффект в виде снижения их регистрируемого количества. Детская порнография, «онлайн-груминг», «кибербуллинг» должны наказываться более сурово, чем сегодня.

Необходимо ужесточение уголовной ответственности за преступления, совершенные группой лиц по предварительному сговору; с использованием искусственного интеллекта и других программ; в отношении лиц с ограниченными возможностями. Целесообразно также введение ответственности за создание, администрирование и финансирование интернет-ресурсов; увеличение наказания за совершение рецидива преступлений против несовершеннолетних с использованием цифровых технологий.

Несомненно, для регулирования вопросов, связанных с безопасным нахождением детей в интернете, требуется разработка специализированных законодательных актов. Для эффективного выявления и удаления противоправного контента в отношении несовершеннолетних необходимо введение жестких норм по регламентации деятельности социальных сетей, видеохостингов и других цифровых сервисов. В связи с чем следует обязать интернет-платформы, осуществлять мониторинг и фильтрацию контента и информировать органы внутренних дел о случаях выявления потенциально опасной информации, направленной против несовершеннолетних.

Трудно переоценить роль органов внутренних дел в предупреждении преступлений против несовершеннолетних. Их деятельность направлена на выявление и раскрытие преступлений против несовершеннолетних, совершаемых с помощью информационно-телекоммуникационных технологий. Данная работа обычно осуществляется путем анализа IP-адресов, блокчейн-транзакций, истории браузеров и переписки включая различные направления от мониторинга интернет-пространства, например, для обнаружения и пресечения онлайн-трансляций сексуального насилия над детьми, противодействия распространения детской порнографии и наконец профилактической работы с провайдерами и

гражданами в целом. За размещение, распространение и хранение материалов, содержащих сцены насилия, сексуальной эксплуатации детей, материалов, подталкивающих несовершеннолетних к суициду и иным противоправным действиям, на наш взгляд, следует рассмотреть вопрос о возможности усиления наказания виновных субъектов.

Кроме того, введение жестких стандартов по защите личных данных несовершеннолетних позволило бы обеспечить их конфиденциальность. В случае нарушения требований предусмотреть применение штрафных санкций вплоть до полной блокировки их деятельности.

Возможно создать единую базу лиц, совершивших преступления в отношении несовершеннолетних в информационно-телекоммуникационной сфере с обязательным введением запрета на их работу как образовательных, так и иных учреждений, связанных с несовершеннолетними. А для ограничения доступа подростков к контенту для взрослых необходимо усовершенствовать систему проверки возраста онлайн-пользователей.

Считаем, что важную роль в этом направлении по предупреждению преступлений против несовершеннолетних с помощью информационно-телекоммуникационных технологий имеет применение современных технологий защиты и контроля, позволяющих блокировать вредоносные программы, фильтровать контент, запрещать вход на нежелательные интернет-ресурсы и др. Например, биометрическая идентификация, основанная на использовании технологии распознавания лица или предъявление электронного удостоверения личности, позволяет при необходимости подтвердить возраст онлайн-пользователя.

Одним из эффективных способов защиты детей в интернете является родительский контроль за несовершеннолетним, когда для входа в социальную сеть или игру нужно обязательное согласие взрослого. Контроль за онлайн-активностью со стороны взрослых, мониторинг их взаимодействия в социальных сетях, ограничение доступа к опасным сайтам и приложениям позволяет реализовать использование специальных программ родительского контроля.

Также достаточно эффективный способ защиты детей в интернете – это образовательный контент. Прохождение специальных курсов по кибер-безопасности на базе образовательных организаций позволило бы и несовершеннолетним, и родителям защитить свою личную информацию, безопасно общаться в онлайн-пространстве, распознать своевременно онлайн-угрозы.

Отдельно отметим вопрос международного сотрудничества в предупреждении IT-преступлений в отношении несовершеннолетних лиц и прежде всего обмен опытом и передовыми технологиями между странами. Для разработки эффективных методов противодействия таким преступлениям, считаем, что все государства должны взаимодействовать между собой, действуя сообща, включая, например, создание платформ для обмена опытом и технологиями, участие в совместных программных инициативах, направленных на защиту детей и подростков в интернет-пространстве, проведение совместных операций против онлайн-мошенников и др. Значительно повышает успешность работы в этом направлении присутствие государственного контроля за функционированием

цифровых ресурсов, обмен информацией о преступниках и существующих цифровых угрозах, основанный на сотрудничестве с международными организациями. Отметим, что для координации усилий по защите детей важную роль должны играть такие организации, как Интерпол и ЮНИСЕФ [1].

Кроме того, необходимо помнить, что реализация указанных правовых мер будет эффективной только при использовании комплексного и скоординированного подхода, в тесном взаимодействии государственных органов, правоохранительных структур, коммерческих и общественных организаций.

Подводя итог вышеизложенному, сделаем следующие выводы.

На данный момент существует острая необходимость совершенствования действующего законодательства. А именно нормативно-правовых актов, регулирующих данную сферу, которые должны своевременно дорабатываться и обновляться и думается предусматривать ужесточение ответственности за преступления против несовершеннолетних.

Для повышения эффективности противодействия преступлениям в рассматриваемой сфере следует проанализировать возможность создания специализированных подразделений киберполиции, специализирующихся на выявлении и расследовании преступлений против несовершеннолетних.

В целях повышения осведомленности населения о рисках в интернет-пространстве крайне необходимо проведение и поддержка информационных компаний для распространения информации через средства массовой информации, социальные сети и образовательные организации.

Для достижения более значимых результатов в предупредительной деятельности необходимо более широко использовать современные технологии обучения, такие как искусственный интеллект и машинное обучение. Применение данных технологий необходимо для анализа сетевого трафика, а также для выявления подозрительных активностей и блокировки противоправного контента путем создания разнообразных фильтров.

Список литературы

1. Баранов А. А. Соломатина Е. А. К вопросу о новых способах совершения и предупреждения IT-преступлений в отношении несовершеннолетних и малолетних // Криминологический журнал. 2024. № 2.
2. Распоряжение Правительства Российской Федерации от 28.04.2023 № 1105 «Об утверждении Концепции информационной безопасности детей в Российской Федерации» // НПП «Гарант-сервис».
3. Обеспечение безопасности детей в сети «Интернет». Детская интернет-безопасность // URL: <https://77.xn--blaew.xn--plai/PAMJATKI/>
4. Безопасность детей в Интернете: как защитить своего ребенка в сети // URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/kids-online-safety>.
5. Безопасная цифровая среда: как защитить ребенка от криминала в сети // URL: <https://xn--80aapampemcchfmo7a3c9ehj.xn--plai/news/bezopasnaya-tsifrovaya-sreda-kak-zashchitit-rebenka-ot-kriminala-v-seti/>.

Григорьев Д. А.¹,
заведующий лабораторией «Криминалистика
и специальная техника», доцент кафедры
государственно-правовых и уголовно-правовых дисциплин
РЭУ имени Г.В. Плеханова,
кандидат юридических наук

Лаптев Д. Д.²,
студент 1 курса, магистерской программы
«Юрист в сфере уголовного судопроизводства»
РГУП имени В.М. Лебедева

СОВРЕМЕННЫЕ МЕХАНИЗМЫ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ВЫЗОВЫ ДЛЯ ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЫ И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Противодействие легализации доходов, полученных преступным путем, с использованием информационно-телекоммуникационных технологий относится к числу наиболее актуальных проблем, выстроенных перед современным российским обществом, а также всей правоохранительной системой. Особая актуальность указанной темы обусловлена тем, что подобные преступные проявления несут колоссальную угрозу национальной безопасности и стабильности финансовой системы Российской Федерации. Более того, в условиях глобализации и цифровизации мировой экономики, исследуемая проблема приобретает транснациональный характер, требуя скоординированных и отлаженных усилий международного сообщества.

Как справедливо отмечает А. И. Бастрыкин, легализация преступных доходов выступает связующим звеном между легальной и нелегальной экономикой, каналом, через который незаконно полученные средства проникают в законную сферу экономических отношений [4]. Соглашаясь с данным мнением, важно отметить, что отмывание преступно полученных доходов, в случае его неэффективного выявления, прямо или косвенно ведет к криминализации легальных секторов экономики. Если говорить простыми словами, то легализация преступных доходов представляет собой процесс, при котором деньги, полученные от незаконной деятельности (например, наркоторговля, коррупция, мошенничество), проходят ряд финансовых операций, чтобы скрыть их криминальное происхождение и придать им видимость законно полученных. Следовательно, преступники получают возможность безнаказанно пользоваться своими незаконными доходами, инвестируя их в легальный бизнес или, например, недвижимость, что подрывает экономическую безопасность, а также искажает рыночную конкуренцию.

¹ © Григорьев Д. А., 2025.

² © Лаптев Д. Д., 2025.

Важно обратить внимание на то, что в условиях стремительного развития информационно-телекоммуникационных технологий происходит трансформация различных механизмов легализации преступных доходов. Таким образом, традиционные схемы отмывания денег дополняются новыми, основанными на использовании цифровых технологий, электронных платежных систем, многообразных криптовалют и анонимных сетей. Данный факт значительно усложняет задачу выявления и пресечения данного вида преступлений правоохранными органами.

Центральным вопросом является определение эффективных механизмов противодействия легализации преступных доходов в условиях цифровизации экономики, а также финансовой системы. Так, для конкретного ответа на данный вопрос необходимо комплексное изучение современных схем отмывания денег с использованием информационно-телекоммуникационных технологий, а также анализ существующих проблем в деятельности правоохранных органов по их выявлению и пресечению.

Определение и основные понятия, связанные с исследуемой категорией преступлений, содержатся в Федеральном законе от 07.08.2011 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [3]. В соответствии со ст. 3 указанного закона, под легализацией (отмыванием) доходов, полученных преступным путем, понимается придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления. Иными словами, отмывание доходов – это определенный процесс, в ходе которого лица маскируют истинное происхождение своих незаконно полученных денежных средств через серию запутанных финансовых операций, чтобы «отмываемые» денежные средства выглядели как полученные из законных источников. Это позволяет им, в свою очередь, использовать такие деньги открыто, не опасаясь привлечения к ответственности или конфискации.

Следует отметить, что существуют и другие подходы к определению данного понятия. Так, в международной практике используется определение, данное в Венской конвенции ООН 1988 г. [1], согласно которой отмывание денег – это конверсия или передача имущества, если известно, что такое имущество получено в результате правонарушения, в целях сокрытия незаконного источника имущества или, оказания помощи любому лицу, участвующему в совершении правонарушения, с тем чтобы оно могло уклониться от ответственности за свои действия.

В современной криминологической науке процесс легализации преступных доходов традиционно рассматривается как состоящий из трех основных этапов [5]:

1. **Размещение** – этап, на котором денежные средства, полученные от преступной деятельности, впервые вводятся в финансовую систему. Например, гражданин Х, получивший крупную сумму наличных денег от незаконной продажи наркотических средств, постепенно вносит их небольшими частями на несколько банковских счетов, открытых на подставных лиц, или приобретает дорогостоящие товары, такие как автомобиль, а также ювелирные изделия, которые

затем можно быстро перепродать. Примечательно, что на данном этапе преступные доходы наиболее уязвимы для выявления.

2. Расслоение – этап, включающий в себя серию операций по переводу средств между различными счетами и финансовыми институтами, как правило, в разных юрисдикциях, с целью сокрытия их происхождения. Например, гражданин X переводит деньги со счетов подставных лиц на счета финансовых компаний в офшорных зонах, которые затем переводят эти средства через ряд других компаний в разных странах, каждый раз меняя валюту и назначение платежа (за консультационные услуги, программное обеспечение или маркетинговые исследования).

3. Интеграция – заключительный этап, на котором средства возвращаются в легальную экономику под видом законно полученных доходов, например, через фиктивные займы, контракты, инвестиции или покупку активов. К примеру, гражданин X получает «займ» от офшорной компании (которую сам же контролирует) для покупки недвижимости или открытия легального бизнеса в России. Впоследствии он возвращает данный «займ» с процентами, тем самым легализуя средства и обосновывая их происхождение.

В практике правоохранительных органов процесс доказывания легализации преступных доходов сопряжен со значительными трудностями. Это неразрывно связано с тем, что особую сложность представляет установление причинно-следственной связи между базовым (предикатным) преступлением и собственно легализацией, ведь совсем не каждая операция с преступно нажитым имуществом преследует цель его легализации [6]. Необходимо доказать, что лицо осознавало преступное происхождение имущества и стремилось придать правомерный вид владению, пользованию и распоряжению им.

Развитие информационно-телекоммуникационных технологий существенно трансформировало механизмы легализации преступных доходов. Наблюдения позволяют сделать вывод о том, что традиционные методы отмыwania денег все чаще дополняются или заменяются новыми схемами, основанными на использовании цифровых технологий. Рассмотрим наиболее распространенные из них.

Электронные платежные системы представляют собой привлекательный инструмент для легализации преступных доходов в силу таких характеристик, как анонимность, трансграничность и высокая скорость проведения операций. Важно отметить, что преступники используют различные схемы с вовлечением электронных кошельков:

– **дробление средств** – разделение крупной суммы на множество мелких переводов между разными электронными кошельками, зарегистрированными на подставных лиц. Например, организованная преступная группа, получившая 10 млн рублей от мошенничества, разделяет эту сумму на 400 переводов по 25 тыс. рублей на различные электронные кошельки, оформленные на граждан из социально уязвимых групп (студентов, пенсионеров, малообеспеченных людей), которые за небольшое вознаграждение предоставили свои паспортные данные. Такое дробление снижает риск обнаружения операций системами финансового мониторинга, после чего средства консолидируются через фиктивные сделки и возвращаются организаторам как «легальный» доход;

– **использование «цифровых мулов»** – привлечение третьих лиц, которые за вознаграждение предоставляют доступ к своим идентифицированным электронным кошелькам для проведения операций. Например, гражданин Х находит граждан, испытывающих финансовые трудности, и предлагает им процент от суммы за использование их кошельков. Через эти кошельки проводятся операции с нелегальными средствами, а сами владельцы кошельков становятся потенциальными фигурантами уголовных или административных дел при выявлении нарушений;

– **создание сети взаимосвязанных электронных кошельков** в различных платежных системах для проведения множественных транзакций с целью запутать следы движения денежных средств. Например, преступная группа создает множество кошельков в разных платежных системах и организуют между ними запутанную цепочку переводов, что затрудняет отслеживание первоначального источника средств.

Наибольшие трудности в выявлении и пресечении легализации преступных доходов возникают при использовании преступниками криптовалют. Как отмечают исследователи, криптовалюты обладают рядом характеристик, делающих их идеальным инструментом для отмыwania денег [7]: децентрализованность – отсутствие единого центра эмиссии и контроля; анонимность – транзакции не привязаны к личности, а только к криптовалютному адресу; трансграничность – переводы не имеют географических ограничений, следовательно, не подпадают под банковское регулирование; необратимость транзакций – невозможность отмены или блокировки операций.

В практике легализации преступных доходов с использованием криптовалют, как правило, можно выделить следующие типичные схемы:

1. **Использование «миксеров» и «тумблеров»** – специализированных сервисов, которые разбивают криптовалютные транзакции на множество мелких, а также перемешивают их с транзакциями других пользователей, что сильно затрудняет отслеживание цепочки операций.

2. **Цепочки обменов** – конвертация преступных доходов в криптовалюту с последующей серией обменов на различные «альткоины» (альтернативные криптовалюты) и обратно, после чего средства выводятся в обычные (национальные) валюты через легальные криптовалютные биржи или через P2P – платформы. Суть заключается в том, что каждая конвертация из одной криптовалюты в другую разрывает цепочку отслеживания движения средств, так как эти операции происходят в разных блокчейн-сетях, что значительно усложняет установление связи между первоначальным источником средств и их конечным получателем.

3. **Использование «анонимных» криптовалют (Monero, Zcash, Dash)**, которые предлагают повышенный уровень приватности по сравнению с Bitcoin, скрывая информацию о сумме транзакции, отправителе и получателе.

4. **Криптовалютные казино и игровые платформы**, которые используются злоумышленниками для конвертации «грязных» денег в «чистые» через имитацию азартных игр и ставок.

Примечательно, что особую опасность среди инструментов легализации преступных доходов представляют ресурсы, функционирующие в скрытом сегменте

интернета. Даркнет – скрытая часть интернета, доступ к которой возможен только через специальное программное обеспечение. Важно заметить, что даркнет предоставляет идеальную среду для совершения противоправных действий в силу обеспечиваемой им анонимности шифрования данных.

В контексте легализации преступных доходов, даркнет используется следующими способами:

1. **Организация торговых площадок** для продажи нелегальных товаров и услуг с оплатой в криптовалюте. Полученные средства затем легализуются через криптовалютные обменники или миксеры.

2. **Предоставление услуг по отмыванию денег** (так называемые «cleaning services»), которые специализируются на маскировке происхождения криптовалютных средств.

3. **Создание мошеннических схем** (фишинг, фейковые инвестиционные платформы), через которые выводятся похищенные средства. Преступники используют анонимность даркнета для создания ресурсов, имитирующих легальные финансовые сервисы, что позволяет им выводить похищенные средства через несколько юрисдикций и конвертировать их в криптовалюту без сохранения цифрового следа, связывающего их с первоначальным преступлением.

Существенным фактором распространения нелегальных финансовых практик являются даркнет-форумы, выступающие в качестве обучающих площадок для обмена опытом в сфере легализации преступных доходов. На подобных ресурсах распространяются детальные инструкции, программное обеспечение или услуги консультантов, специализирующихся на обходе систем финансового мониторинга. Это создает эффект мультипликации преступных навыков, когда технологии отмывания денег становятся доступными даже для лиц, не обладающих глубокими техническими знаниями.

Как показывает практика, успешные операции правоохранительных органов по ликвидации крупных даркнет-площадок (Skilk Road, AlphaBay, Hansa) дают лишь временный эффект, поскольку на их месте быстро появляются новые, с усовершенствованными механизмами анонимизации и безопасности.

Игровой бизнес традиционно является одной из сфер, используемых для отмывания денежных средств. Так, с развитием онлайн-гемблинга возможности для легализации преступных доходов значительно расширились. В цифровой среде используются следующие схемы:

1. **Размещение «грязных» денег на счетах онлайн-казино** с последующим осуществлением минимального количества ставок для создания видимости игровой активности и последующим выводом средств как выигрыша.

2. **Использование «казино-однодневок»**, специально созданных для целей отмывания денег, которые после проведения необходимых операций ликвидируются.

3. **Манипуляции с игровыми аккаунтами**, когда один и тот же игрок контролирует несколько аккаунтов и организует между ними перевод средств под видом проигрышей и выигрышей.

4. **Интеграция криптовалютных платежей** в онлайн-казино, что добавляет дополнительный слой анонимности к операциям.

Усугубляет ситуацию отсутствие эффективного международного регулирования онлайн-гемблинга, позволяющее организовывать виртуальные игровые заведения в юрисдикциях с минимальным надзором за финансовыми потоками. Такие операторы нередко регистрируются в офшорных зонах, предоставляют услуги по всему миру, но фактически не подчиняются требованиям национальных систем финансового мониторинга, что создает идеальные условия для легализации преступных доходов.

Особенно сложным для выявления являются комбинированные схемы легализации, когда цифровые методы совмещаются с традиционными. Практика показывает, что наиболее распространенными являются следующие комбинации:

1. Использование подставных компаний с элементами цифрового мошенничества – создание фиктивных фирм, через которые проходят операции с использованием криптовалют или электронных платежных систем, с последующей имитацией деятельности в сфере, например, консалтинга, IT-услуг или цифрового маркетинга.

2. «Смурфинг» с цифровым компонентом – координация через защищенные мессенджеры сети физических лиц (так называемых «смурфов»), которые осуществляют множественные мелкие операции с криптовалютами или электронными кошельками с последующим объединением средств.

3. Инвестиционные схемы – создание псевдо-инвестиционных платформ, особенно в сфере стартапов, блокчейн-проектов или NFT токенов, где «грязные» деньги вкладываются под видом легальных инвестиций, а затем выводятся как прибыль.

4. Интеграция с традиционными офшорными схемами – использование классических офшорных юрисдикций в комбинации с криптовалютными операциями для создания многослойных структур, затрудняющих отслеживание происхождения средств.

Как показывает анализ выявленных схем, преступники постоянно адаптируют и совершенствуют методы легализации, быстро реагируя на изменения в законодательстве и технологической среде. Это создает серьезные вызовы для правоохранительной системы в деле противодействия отмыванию преступных доходов.

Анализируя современное состояние противодействия легализации преступных доходов с использованием информационно-телекоммуникационных технологий, можно выделить ряд ключевых вызовов, с которыми сталкивается правоохранительная система Российской Федерации [8]. Стоит отметить, что данные вызовы значительно снижают эффективность борьбы с легализацией преступных доходов.

Так, одной из основных проблем является технологический разрыв между возможностями преступников и правоохранительных органов. Это неразрывно связано с тем, что большинство подразделений, занимающихся противодействием легализации преступных доходов, не имеют специализированных программных обеспечений для непосредственного анализа блокчейн-транзакций и отслеживания криптовалютных переводов. Также стоит отметить, что наблюдается нехватка специализированных специалистов с компетенциями в области

информационных технологий, блокчейна, криптографии, а также цифровой криминалистики. Усугубляет ситуацию тот факт, что высоквалифицированные IT-специалисты зачастую предпочитают трудоустройство в коммерческом секторе или, что более тревожно, оказываются вовлечены в противоправную деятельность, где их навыки вознаграждаются значительно более высокими гонорами, чем может предложить государственная служба. Таким образом, создается порочный круг, когда наиболее компетентные специалисты оказываются «по другую сторону», еще сильнее увеличивая технологический разрыв между возможностями криминальных структур и правоохранительных органов.

Особую сложность представляет трансграничный характер легализации преступных доходов с использованием цифровых технологий. Данные о транзакциях, серверы и организаторы схем легализации могут находиться в различных юрисдикциях, что требует сложных процедур международной правовой помощи. Различия в национальных законодательствах создают «серые зоны», которые активно используются преступниками.

Правовая неопределенность статуса криптовалют и иных виртуальных активов создает сложности в квалификации преступлений, связанных с их использованием. Существенным препятствием является несовершенство законодательства о доказательствах в контексте цифровых следов и электронных данных, что приводит к проблемам с процессуальным закреплением результатов оперативно-розыскной деятельности [9].

Важно учитывать тот факт, что эффективное противодействие легализации преступных доходов требует скоординированных действий различных государственных органов, однако наблюдается ведомственная разобщенность, а также отсутствие единой системы информационного обмена между Росфинмониторингом, ФНС России, ЦБ РФ, МВД России, ФСБ России и Следственным комитетом. Сложившаяся ситуация усугубляется недостаточной регламентацией механизмов межведомственного взаимодействия в сфере противодействия легализации доходов, полученных преступным путем с использованием новых информационных технологий [10].

Указанные вызовы требуют комплексного подхода к совершенствованию системы противодействия легализации преступных доходов с использованием информационно-телекоммуникационных технологий. Необходимы разработка и реализация согласованной стратегии, учитывающей как перспективные направления технологического развития, так и усовершенствование методов, а также способов отмыwania денег в цифровой среде. Вместе с тем особого внимания заслуживает создание адаптивных механизмов правового регулирования, способных оперативно реагировать на появление новых схем легализации преступных доходов без необходимости глобального пересмотра нормативной правовой базы.

В свою очередь, анализ международного опыта противодействия легализации преступных доходов с использованием цифровых технологий демонстрирует эффективность комплексного подхода. Группа разработки финансовых мер борьбы с отмыwанием денег (ФАТФ) регулярно обновляет стандарты в отношении вир-

туальных активов, предусматривая идентификацию клиентов, мониторинг операций, лицензирование сервисов и обмен информацией о транзакциях. Многие страны внедряют специализированные подходы, например, США создают профильные подразделения и используют аналитическое ПО для анализа блокчейн-транзакций, ЕС формируют централизованные реестры и механизмы превентивной заморозки средств, а Япония применяет систему лицензирования и аудита криптобирж. Иными словами, мировая практика подтверждает необходимость сочетания государственного регулирования, саморегулирования участников рынка и международного сотрудничества через структуры Egmont Group, Интерпола и Европола с целью эффективного противодействия транснациональным схемам отмывания денег [11].

На основе проведенного исследования можно предложить следующие пути совершенствования системы противодействия легализации преступных доходов. Эффективное решение обозначенной проблемы требует комплексного подхода, который будет учитывать стремительное развитие информационно-телекоммуникационных технологий.

В сфере нормативно-правового обеспечения необходима разработка специального законодательства о регулировании криптовалют и виртуальных активов с четким определением их правового статуса. Требуется совершенствование процедур сбора, а также использования цифровых доказательств, включая данные блокчейн-анализа. Целесообразно внедрить концепции «следования за деньгами», предусматривающей упрощенные процедуры конфискации подозрительных активов. Важную значимость приобретает задача адаптировать отечественное законодательство к международным стандартам ФАТФ в области борьбы с отмыванием денег.

Авторам представляется, что преодоление технологического разрыва между возможностями преступников и правоохранительных органов требует создания единой системы мониторинга криптовалютных транзакций, совмещенный с Росфинмониторингом. Так, перспективным направлением является создание специализированных программных обеспечений (например, на основе искусственного интеллекта), благодаря которым будет возможно выявление подозрительных операций. Также необходимо формирование централизованной базы данных подозрительных цифровых идентификаторов, что позволит оперативно блокировать попытки легализации преступных доходов в цифровой среде.

В организационном аспекте целесообразно формирование специализированных подразделений по расследованию цифровых финансовых преступлений, разработка регламентов взаимодействия между ведомствами, развитие кадрового потенциала, а также активизация международного сотрудничества в сфере противодействия современным схемам легализации преступных доходов.

Подводя итог проведенного исследования, следует отметить, что легализация преступных доходов с использованием информационно-телекоммуникационных технологий представляет собой серьезную угрозу экономической безопасности государства. Современные схемы отмывания денег характеризуются высоким уровнем сложности, трансграничным характером и активным использованием цифровых технологий, что значительно затрудняет их расследование.

Преступники успешно адаптируют новейшие информационные технологии для создания многоуровневых схем легализации, используя криптовалюты, электронные платежные системы, даркнет-платформы, а также иные инструменты цифровой экономики. Более того, особую опасность представляют комбинированные схемы, совмещающие традиционные методы отмывания денег с цифровыми технологиями.

Правовое противодействие исследуемым явлениям осуществляется в рамках уголовного законодательства. Статья 174 Уголовного кодекса Российской Федерации (далее – УК РФ) устанавливает ответственность за легализацию (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем, а статья 174.1 УК РФ предусматривает ответственность за легализацию средств или имущества, приобретенных лицом в результате совершения им преступления. Примечательно, что санкции за данные преступления включают штрафы в размере до одного миллиона рублей, лишение свободы на срок до семи лет со штрафом, а при совершении преступления организованной группой или в особо крупном размере – лишение свободы на срок до десяти лет со штрафом и с ограничением свободы (например, запретом занимать определенные должности или заниматься определенной деятельностью в финансовой сфере).

Однако эффективность правоприменения в данной сфере сталкивается с рядом проблем, включая технологический разрыв между возможностями преступников и правоохранительных органов, недостаточную квалификацию специалистов, несовершенство законодательства в области регулирования цифровых технологий и ведомственную разобщенность. В условиях постоянного совершенствования преступных схем наказания, предусмотренные действующим законодательством, не всегда соразмерны причиняемому ущербу, а сам процесс доказывания подобных преступлений остается крайне сложным.

Для повышения эффективности противодействия легализации преступных доходов необходим комплексный подход, о котором говорилось ранее, включающий совершенствование нормативно-правовой базы, развитие технологического потенциала правоохранительных органов, оптимизацию организационных механизмов межведомственного взаимодействия, а также развитие кадрового потенциала. Особое внимание следует уделить усилению ответственности за использование сложных цифровых инструментов для легализации преступных доходов и введению дополнительных квалифицирующих признаков, учитывающих специфику современных технологических способов отмывания денег.

Размышляя над перспективными направлениями совершенствования системы противодействия легализации незаконно полученных доходов, следует отметить, что успешное решение проблемы противодействия легализации преступных доходов с использованием информационно-телекоммуникационных технологий невозможно без международного сотрудничества и координации усилий всех заинтересованных сторон. Таким образом, только комплексный подход позволит обеспечить защиту экономических интересов государства и общества в условиях цифрового изменения финансовой системы.

Список литературы

1. Венская конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ (Заключение в г. Вене 20.12.1988) // Сборник международных договоров СССР и Российской Федерации. Вып. XLV VII. М., 1994. С. 133–157.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) // Собрание законодательства РФ, 17.06.1996. – № 25. ст. 2954.
3. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Собрание законодательства РФ. 2001. – № 33 (ч. 1). – Ст. 3418.
4. Бастрыкин А. И. Бастрыкин: бороться с экономическими преступлениями должно одно ведомство // Право.ру. URL: <https://pravo.ru/news/view/23509/>.
5. Иванов П. И. Стадии и способы легализации преступных доходов, полученных в результате совершения преступлений экономической и налоговой направленности // Вестник Санкт-Петербургского университета МВД России. 2020. № 3 (87). С. 148–156.
6. Пушкарев В. В., Толоков А. В. Основы организации противодействия преступлениям, совершенным с использованием криптовалют // Вестник экономической безопасности. 2023. № 4. С. 88–92.
7. Холин А. Н. Пути совершенствования организационно-правовых мер по борьбе с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма // Научный журнал. 2023. № 12 (69). С. 27–37.
8. Барсэл И. В. Актуальные проблемы противодействия легализации доходов, полученных преступным путем // Юридическая наука. 2023. № 2. С. 87–90.
9. Кузьминова О. А., Ермейкина К. А. Противодействие отмыванию (легализации) доходов, полученных преступным путем в обеспечении финансовой устойчивости государства // Столыпинский вестник. 2023. № 5. С. 2373–2383.
10. Чупрова А. Ю. Перспективы противодействия легализации преступных доходов в цифровую эпоху // Уголовное право. 2023. № 3. С. 112–119.
11. Иванов П. И. Проблемы противодействия легализации преступных доходов и пути их решения // Вестник Белгородского юридического института МВД России имени И.Д. Путилина, 2020.

Ерлан Б. Т.¹,
*старший преподаватель Института
 повышения квалификации Министерства
 внутренних дел Республики Узбекистан, PhD*

ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРЕДУПРЕЖДЕНИИ СОВРЕМЕННЫХ УГРОЗ

Все мы привыкли использовать интернет в повседневной деятельности. Поиск информацию в сети Интернет осуществляется с использованием различных электронных устройств, имеющей в своем составе управляющую систему этого цифрового устройства – операционную систему, компьютеры и мобильные устройства, читаем, загружаем и сохраняем нужную информацию. При осуществлении этой деятельности мы используем интернет-сервисы и ресурсы, которые выполняют функции хранения, предоставления, визуализации и передачи контента. Угрозы нашей безопасности возникают в результате того, являются ли эти интернет-сервисы и источники искомого контента действительно безопасными или нет.

При использовании сети соблюдается и выполняется разработанные требования безопасности при использовании сети Интернет. Из этих самыми основными требованием является то, чтобы не загружать зараженный вирусом вредоносный контент, который при запуске содержимого выполняет вредоносные действия в этой системе в интересах хакера. С выполнением таких мер обеспечивается безопасность системы.

В настоящее время в средствах массовой информации все большую популярность приобретают термины «кибербезопасность», «кибератака», «киберугрозы» и «хакерство». Эти понятия используются вместе с понятием информационной безопасности. Это требует различения двух понятий, которые должны объяснить суть вредоносных действий в области информационных технологий.

Научное обоснование использования этих терминов также считается неоднозначным. Изучая понятие кибербезопасность, мы видим, что этот термин состоит из двух частей, это термины «кибер» и «безопасность».

Слово «кибер» происходит от слова кибернетика (др.-греч. Κυβερνήτιχη – искусство управления судами) – это понятие ввел в науку французский ученый, физик, математик Андре-Мари Ампер в 1834 г., назвав кибернетику «эффективным управлением» [1]. Это понятие в значительной степени связано с системой государственного управления, благодаря которой управление может быть легко осуществлено государством, основанным на этой кибернетической точки зрения, для создания лучших условий проживания для своих граждан.

После этого в 1948 г. американский ученый-математик, основатель кибернетики и искусственного интеллекта Норберт Винер впервые предложил кибернетику как современную науку [1]. В этом случае кибернетика включает изучение

¹ © Ерлан Б. Т., 2025.

черного ящика и аналогичных систем, а также обратной связи, возникающей в системе управления, коммуникации и самоорганизации в живых организмах, машинах и организациях. Кибернетика фокусируется на том, как система (цифровая, механическая или биологическая) обрабатывает любую информацию, обрабатывает информацию, которая представляет собой две задачи, возложенные на нее, либо в результате изменения ее состава или функции в результате реакции на это информационное воздействие, либо в результате изменения части системы в результате других воздействий, который позволить системе лучше выполнять задачи по реагирования на это воздействие [1].

Слово «безопасность системы» или «уровень безопасности» системы является общим показателем, оценивающей воздействий будущему существованию любой системы, ее выживанию в будущем.

Слово «кибер» обозначает эффективное управление в произвольной материальной, живой и нематериальной системе. В любой системе, когда его управление приводит к полезному или вредному результату, это оценивается, что система готов существованию, выживанию в будущем или требуется исчезновению этой системы, ее выходу из строя. При оценке выполнение задач поставленные перед отдельными ее под системными частями, являющимися компонентами этой системы считается эффективными, полезными в управлении то это система с точки зрения кибербезопасности обеспечен.

При выявлении системой несовершенных подсистем и выполняя процедуры удалении этих подсистем или качественное усовершенствование подсистем позволяет в дальнейшем выполнении функций всей системы считается, что кибербезопасность этой системы обеспечена.

Вместе с тем понятие системы тоже является ключевым. Слово «система» происходит от латинского «*Systema*», древнегреческого «*σύστημα*», что означает «целое множество, состоящее из нескольких компонентов (элементов); сумма». Система – это совокупность простых элементов как единого целого, взаимосвязанного по определенным правилам для достижения единой цели. Каждый простой элемент в наборе также может быть системой в свою очередь. Совокупность объектов тоже является системой при выполнении функций для достижения единой цели.

В информационных системах функционирующих в интернете сервисах задачей является предоставления интересного контента и внедрение рекламы. При выполнении этих задач если источник контента выполняет и другие цели, например, распространяет зараженный контент преднамеренно или ввиду некомпетентности непреднамеренно в обоих случаях этот система обречен провалу, т. е. из-за необеспеченности кибербезопасности это система потеряет подписчиков и в будущем перестает существовать.

Понятие кибербезопасности применяется к системе управления системой. Кибербезопасность – это наука, которая изучает как полезные, так и вредные эффекты, которые могут повлиять на общую часть управления любой системой, чтобы гарантировать ее существование в будущем.

В настоящее время кибербезопасность стала важной функцией цифровых электронных систем. Становление важной особенностью, в свою очередь, объясняется тем, что увеличивается количество способов дистанционного взаимодействия по сети с любыми цифровыми системами, даже эти вредоносные воздействия вызывают сбой системы, прекращение ее функционирования (исчезновение), изменение ее функционирования (модификация) или переориентацию системы на совершенно другую цель (redirect).

До сих пор в литературе понятие информационной безопасности широко используется и в научной сфере. Три основных принципа информационной безопасности они направлены на обеспечение конфиденциальности информации (Confidentiality), целостности информации (Integrity) и постоянной готовности информации к использованию (Availability) [2, 3]. Основным объектом информационной безопасности является передаваемая или обрабатываемая информация.

Из этого можно сделать вывод, что использование понятия информационной безопасности при обеспечении безопасности объектов, организованных из сложных систем, не является эффективным, и более эффективным является применение к системе дополнительных понятий, а не информации как основного объекта. По этой причине концепция кибербезопасности является оптимальной парадигмой для сложных систем. Основным объектом кибербезопасности являются целые информационные системы, которые и применяются и к другим объектам.

Объектом информационной безопасности является «информация», объектом кибербезопасности – «система». Существующие в настоящее время угрозы информационных технологий не может полностью объясниться через понятие информационной безопасности, финансирование преступлений с помощью криптовалют, захват информации с помощью социальной инженерии, мошенничество с помощью «fishing-smishing-voicemishing-farming», угрозы связанные с банковскими картами, воздействие деятельности системы, организации или личности, то есть распространение «фейковых» сообщений, «deepfake» подготовка и распространение информации, вредной для деятельности личности, общества и государства, в социальных сетях, создание секретных групп в социальных сетях, незаконное владение информационных объектов через ботнеты. Объяснение этих вредоносных информационных явлений с помощью концепции кибербезопасности является эффективным.

В обеспечении информационной безопасности большое значение имеет и обеспечение кибербезопасности. человек или предприятие подвергаются кибератаке deepfake. Deepfake – это угроза жизни реального человека путем создания его цифрового имиджа с использованием информационных технологий и, таким образом, распространения ложной информации о личности. В этом случае целостность, конфиденциальность и доступность информации не нарушена с точки зрения информационной безопасности. С точки зрения кибербезопасности, deepfake влияет на этого человека на его жизнедеятельность. Наносит ущерб социальным, экономическим и жизненным интересам человека. А распространение этой ложной deepfake информации в интернете информационной системой, каналом блогера или

источником мультимедийного контента типа инстаграмм, тик-ток или youtube поставить в сомнение этих систем и снизить рейтинг этих информационных систем, которые будет влиять на его существование в будущем.

Таким образом, оценка кибератаки *deepfake* с точки зрения кибербезопасности будет иметь более научную основу, чем оценка *deepfake* с точки зрения информационной безопасности.

Принимая во внимание классическое понятие компьютерных вирусов с точки зрения информационной безопасности [4], для объяснения нарушения целостности, конфиденциальности и доступности передаваемой информации требуется более широкое объяснение, использование дополнительных терминов.

С точки зрения кибербезопасности научное объяснение приводится к тому, что компьютерная система управления – операционная система – является объектом и предназначена для выполнения своих функций. Но из-за имеющегося недостатка в его объекте, а точнее из-за несовершенства его управления, эта операционная система не сможет выполнять свою функцию в результате заражения вирусом. В результате выживание этой системы, т. е. использование этой операционной системы-объекта в будущем, будет пересмотрено в связи с недостаточной кибербезопасности.

Заключение.

В современном мире информационные системы для жизни общества стали важной и неотъемлемой частью, что выдвигает их на первый план по обеспечению кибербезопасности. Для государства и общества становится необходимым в доступности этих информационных систем, что требует тратить ресурсы на обеспечение кибербезопасности. Расходуемые ресурсы подразделяются на материальные, научные и человеческие. Человеческие ресурсы связаны с уровнем образования и означают, что в этой области должны работать специалисты, знающие суть проблем кибербезопасности и пути их решения.

Список литературы

1. Wiener N . Cybernetics or Control and Communication in the Animal and the Machine. New York : The Technology Press and John Wiley & Sons, Inc. Paris : Hermann et Cie, 1948.
2. Борьба с преступностью в киберпространстве: проблемы и решения, сборник материалов Республиканской научно-практической конференции, Академия МВД РУ (24.02.2022). Ташкент : MALIK PRINT Co., 2022.
3. Акбаров D. E., Криптографические методы обеспечения информационной безопасности и их применение. Ташкент : O‘zbekiston markasi, 2009.
4. Акбаров D. E, Мусаев А. И. Исследование основ существующих алгоритмов поточного шифрования и их классификация. Ташкент : Axborotkommunikatsiyalar: tarmoqlar, texnologiyalar, yechimlar, “UNICON.UZ”, 2009. С. 36–45.

Калашников И. В.¹,
 заместитель начальника кафедры
 криминологии Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат юридических наук, доцент

Скворцова К. Р.²,
 курсант ИПСОПР
 Московского университета
 МВД России имени В.Я. Кикотя

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРЕДУПРЕЖДЕНИЯ И ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Сегодня киберпреступность остается одной из наиболее острых угроз безопасности для общества и государства. По данным МВД России, за последние годы масштабы киберпреступлений значительно возросли, и их количество продолжает расти. [1, с.101]. В январе–декабре 2024 г. зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8 % в январе-декабре 2023 г. до 40,0 %.

Практически все такие преступления (98,7 %) выявляются органами внутренних дел. Почти половина таких преступлений (48,2 %) относится к категориям тяжких и особо тяжких (369,3 тыс.; +7,8 %), четыре преступления из пяти (84,8 %) совершаются с использованием сети Интернет (649,1 тыс.; +23,2 %), почти половина (45,2 %) – средств мобильной связи (346,0 тыс.; +14,3 %). Почти две трети таких преступлений (63,5 %) совершается путем кражи или мошенничества: 486,3 тыс. (+2,3 %), почти каждое восьмое (12,4 %) – с целью незаконного производства, сбыта или пересылки наркотических средств: 94,6 тыс. (+16,1 %) [2, с. 3].

С развитием цифровых технологий защита информационной инфраструктуры стала одной из ключевых задач национальной безопасности. В России одной из основополагающих мер по защите информационной среды является Доктрина информационной безопасности, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Этот документ закрепляет принципы и цели информационной политики, определяя меры, направленные на защиту как гражданских, так и государственных информационных ресурсов от угроз, связанных с киберпреступностью и иностранным вмешательством. Доктрина обозначает, что основные угрозы кибербезопасности связаны с воздей-

¹ © Калашников И. В., 2025.

² © Скворцова К. Р., 2025.

ствием на критически важную информационную инфраструктуру и распространением вредоносных программ, способных нанести вред экономике и национальной безопасности.

В рамках Доктрины информационной безопасности установлены приоритеты государственной политики, которые включают:

1. Защиту персональных данных граждан и конфиденциальной информации государственных органов.
2. Разработку и внедрение систем киберзащиты, способных противостоять новым видам киберугроз.
3. Укрепление межведомственного взаимодействия и усиление международного сотрудничества в сфере кибербезопасности.
4. Обучение и повышение квалификации кадров, отвечающих за защиту информации [6].

Наряду с Доктриной информационной безопасности, в России разработаны и действуют федеральные законы, регулирующие вопросы кибербезопасности. К ключевым нормативным актам относятся:

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который определяет основы правового регулирования информационных отношений, правила сбора и хранения данных, а также меры по защите персональных данных.

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который регулирует вопросы защиты важнейших объектов инфраструктуры, от которых зависит функционирование государства и общества. Согласно закону организации, работающие с критически важной информационной инфраструктурой (КИИ), обязаны принимать меры для предотвращения несанкционированного доступа к своим информационным системам, обеспечивать защиту информации и контролировать угрозы кибератак.

Кроме того, Федеральный закон в ред. от 08.08.2024 № 152-ФЗ «О персональных данных» закрепляет правила обработки и защиты персональных данных граждан, обязывая организации разрабатывать и внедрять меры по их защите. Нарушение законодательства влечет за собой административную и уголовную ответственность, включая штраф и возможную приостановку деятельности нарушителя. Эти законы помогают усилить контроль над обработкой данных, уменьшить вероятность утечек и предотвратить неправомерное использование персональной информации.

В рамках обеспечения информационной безопасности российские законодатели также разработали программу «Цифровая экономика Российской Федерации», утвержденную постановлением Правительства РФ от 28 июля 2017 г. № 1632-р [9]. Эта программа направлена на развитие инфраструктуры цифровой экономики, создание условий для безопасного функционирования информационных систем и формирование устойчивой цифровой среды. Среди приоритетных направлений программы – разработка отечественных программных реше-

ний для защиты данных и информационной инфраструктуры, создание национальных систем мониторинга и обнаружения киберугроз, а также обеспечение доступности образовательных программ в области кибербезопасности.

Программа «Цифровая экономика» ориентирована на создание комплексной системы защиты информации, включающей как государственные, так и частные информационные структуры. В рамках программы предусматриваются следующие меры:

1. Развитие национальных технологий кибербезопасности, способных конкурировать с зарубежными решениями.
2. Поддержка отечественных разработчиков программного обеспечения для киберзащиты.
3. Создание центров обработки данных с высоким уровнем защиты от кибератак.
4. Реализация образовательных программ в Российской Федерации и повышение квалификации специалистов в области ИТ и информационной безопасности.

Одним из ключевых аспектов эффективного противодействия киберпреступности в Российской Федерации является межведомственное взаимодействие между различными государственными структурами: МВД России, ФСБ России, Роскомнадзора и другими ведомствами, координирующими свои усилия для защиты информации и предотвращения киберугроз. Совместная работа между ведомствами позволяет оперативно обмениваться информацией о возникающих угрозах, предотвращать кибератаки и расследовать инциденты.

Важной частью работы по повышению уровня защиты также является подготовка квалифицированных кадров, способных оперативно реагировать на киберугрозы. В России активно развиваются программы обучения специалистов в области кибербезопасности, как в государственных учебных заведениях, так и на базе частных компаний. Повышение квалификации и обучение специалистов в сфере информационной безопасности включены в национальные программы, что позволяет формировать высококвалифицированные кадры для работы в этой области.

Международное сотрудничество и опыт зарубежных стран играет весомую роль международного сотрудничества в борьбе с киберпреступностью.

Проблема киберпреступности является глобальной, и ее решение требует совместных усилий государств. Одной из важнейших международных инициатив в этой области стала Конвенция о киберпреступности Совета Европы (Будапештская конвенция), подписанная в 2001 г. [8]. Конвенция является первым и пока единственным международным документом, устанавливающим стандарты для расследования и пресечения киберпреступлений. Она обязывает страны-участницы создать правовые условия для эффективного расследования кибератак и обмена данными между правоохранительными органами. Несмотря на то, что Россия не присоединилась к конвенции, она признает ее важность и предпринимает шаги для улучшения международного сотрудничества.

Взаимодействие России с другими странами в области борьбы с киберпреступностью осуществляется в рамках двусторонних и многосторонних соглаше-

ний. Россия активно сотрудничает с Китаем, Индией и странами СНГ, разрабатывая совместные механизмы реагирования на киберугрозы. Важной платформой для такого сотрудничества стал Соглашение о сотрудничестве государств СНГ в борьбе с преступлениями в сфере компьютерной информации, подписанное в 2001 г. В рамках соглашения участники обмениваются данными о кибератаках и согласовывают действия по расследованию инцидентов.

Ряд международных организаций также играет значительную роль в координации усилий по борьбе с киберпреступностью.

Исходя из вышеизложенного, основными тенденциями киберпреступлений выступают:

- прослеживается связь между высокой интенсивностью кибератак и международной политической обстановкой;
- имеет высокий уровень латентности;
- рост доли мошенничеств в структуре киберпреступности;
- доступность информации о способах совершения киберпреступлений;
- увеличении доступности технологий, позволяющих совершать киберпреступления.

Также можно отметить, что прогнозируется рост числа киберпреступлений.

Список литературы

1. Криминологическая характеристика и прогнозирование отдельных видов киберпреступлений, совершаемых в информационно-телекоммуникационном пространстве на территории Российской Федерации / Калашников И. В., Калашникова Л. Н. // Криминологический журнал. 2024. № 2. С. 101–106.
2. Сборник Состояние преступности в России за январь–декабрь 2024 года. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2024 года.
3. Криминология / Аванесов Г. А., Антонян Е. А., Иванцов С. В. и др. (Восьмое издание, переработанное и дополненное). М., 2023.
4. Личность преступника, совершающего преступления в сфере экономики с использованием информационно-телекоммуникационных технологий / Калашников И. В. // В сборнике: Актуальные вопросы предупреждения преступлений в сфере информационно-телекоммуникационных технологий: криминологический и виктимологический аспекты. Всероссийская научно-практическая конференция: сборник научных трудов / Сост. Е. Е. Колбасина. М., 2022. С. 46–49.
5. Доклад Генерального Секретаря ООН «Воздействие организованной преступной деятельности на общество в целом» // Материалы комиссии ООН по предупреждению преступности и уголовному правосудию. Вена, L7CN 15/1993/3.
6. Доктрина информационной безопасности РФ, утвержденная Указом Президента Российской Федерации от 09.09.2000 № Пр-1895 // Российская газета. 2000. 28 сентября. № 187.
7. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

Российской Федерации: утверждена Указом Президента Российской Федерации от 12.12.2014 № К 1274 // URL: <https://base.garant.ru/71127868>.

8. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.).

9. Противодействие использованию ИТТ в преступных целях: доклад Генерального секретаря ООН, подготовленный в соответствии с Резолюцией 73/187 Генеральной Ассамблеи ООН 03.07.2019 // URL: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf.

10. Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы "Цифровая экономика Российской Федерации"» // НПП «Гарант-сервис».

11. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 08.01.2025) // СПС «Консультант-Плюс».

Колбасина Е. Е.¹,
доцент кафедры криминологии
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

Василенко Д. И.²,
курсант международно-правового факультета
Московского университета
МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИИ В ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ: МЕХАНИЗМЫ, УГРОЗЫ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

Технология распределенного реестра, широко известная как блокчейн, прочно утвердилась в качестве одного из ключевых направлений современных IT-разработок. Концептуально она возникла параллельно с идеями криптовалют и криптографических кошельков ориентировочно в 2008 г. Именно блокчейн изначально обеспечил цифровым активам такие важные свойства, как конфиденциальность переводов, высокую скорость обработки транзакций, децентрализованную архитектуру управления и гарантии неизменности (защиту от фальсификации) зарегистрированных операций.

Первые теоретические основы подобной криптографической системы были заложены еще в 1982 г. Дэвидом Чаумом в рамках его диссертационного исследования, практическая реализация состоялась позже. После ряда доработок и модификаций, предложенных другими исследователями, первая функционирующая децентрализованная блокчейн-система была представлена и внедрена в 2008 г. анонимной персоной (или коллективом) под псевдонимом Сатоши Накамото. Эта реализация стала краеугольным камнем для биткоина, а затем и для множества других криптовалютных активов [1].

Механизм блокчейна предполагает генерацию уникального хэш-кода для каждого блока данных, что обеспечивает неповторимость и подтверждает подлинность каждого элемента цепи. Эта же характеристика уникальности переносится и на транзакции, проводимые с использованием криптовалют. Л. Г. Ефимова поясняет природу владения биткоином: это необладание им в физическом смысле, а, скорее, наличие в распределенном цифровом журнале записи о переводе биткоинов на ваш уникальный адрес [4]. Следовательно, фундаментальными чертами сделок на базе блокчейна выступают отсутствие центрального контрольного органа и уникальность каждой операции, подтверждаемая ее неповторимым идентификатором.

¹ © Колбасина Е. Е., 2025.

² © Василенко Д. И., 2025.

Как и любая сложная система, блокчейн имеет свои достоинства и уязвимости. Существенным фактором риска остается человеческий элемент – психофизиологические аспекты поведения людей, которые сложно полностью учесть при проектировании системы и которые могут привести к непредвиденным сбоям. К таким аспектам относится, например, стремление к быстрой выгоде («легким деньгам»), побуждающее осведомленных пользователей искать лазейки в системе для обхода механизмов безопасности. Помимо этого, важно осознавать, что технология блокчейн может применяться не только в рамках правового поля, но и для осуществления нелегальных операций.

Блокчейн-технологии, изначально задуманные как инструмент для повышения прозрачности и безопасности транзакций в цифровой экономике, сегодня демонстрируют двойную природу. Наряду с легитимным применением в финансах, логистике, здравоохранении и других отраслях, блокчейн становится инструментом для осуществления преступной деятельности, что ставит под угрозу стабильность и доверие к новым технологиям. Сложность отслеживания транзакций, анонимность и децентрализованный характер блокчейна привлекают преступников, стремящихся к сокрытию своих незаконных операций [2].

Данное исследование направлено на анализ механизмов использования блокчейна в преступных целях, выявление основных угроз, а также изучение и оценку эффективности существующих и потенциальных стратегий противодействия. Цель исследования – разработка рекомендаций по минимизации рисков, связанных с преступным применением блокчейн-технологий.

В процессе исследования использованы следующие методы: обзор научной литературы и аналитических отчетов международных организаций, анализ реальных кейсов преступлений, совершенных с использованием блокчейна, сравнительный анализ мер регулирования, применяемых в различных странах. Также проведен анализ данных, полученных из открытых источников, таких как отчеты правоохранительных органов и специализированных компаний, занимающихся блокчейн-аналитикой (Chainalysis, CipherTrace).

Основные принципы блокчейна, такие как децентрализация, псевдоанонимность и неизменяемость данных, обеспечивают высокую степень защиты от цензуры и несанкционированного доступа [4]. Однако эти же характеристики могут быть использованы в преступных целях. Децентрализация затрудняет контроль и регулирование транзакций, а псевдоанонимность, хотя и не гарантирует полной анонимности, усложняет идентификацию участников транзакций. Неизменяемость данных, с одной стороны, обеспечивает сохранность информации, а с другой – затрудняет удаление или изменение незаконных транзакций.

Блокчейн широко используется в различных сферах, включая финансы, логистику, здравоохранение (хранение медицинских данных) и голосование (обеспечение прозрачности выборов). Однако каждая из этих сфер имеет свои потенциальные уязвимости. Например, в сфере криптовалют уязвимостями являются хакерские атаки на криптобиржи, фишинговые атаки и мошеннические схемы. В логистике уязвимостью может быть подделка данных о происхождении товара.

Криптовалюты являются распространенным средством для отмыwania денег, которые были получены преступным путем. Преступники используют разнообразные методы, чтобы замаскировать денежные средства под общий поток денег: использование миксеров (сервисов, которые скрывают источник транзакций), транзакции через целый ряд. Криптовалютный рынок привлекает мошенников, которые могут предложить инвестиции в несуществующие проекты, которые «гарантируют» высокую прибыль. Примеры таких схем включают OneCoin и Bitconnect, которые смогли обмануть инвесторов на миллиарды долларов. Криптовалюты могут быть использованы для финансирования террористических организаций, поскольку они позволяют переводить средства анонимно и без контроля со стороны финансовых институтов, то есть децентрализованно.

Даркнет-маркетплейсы, такие как Silk Road и Hydra, использовали криптовалюты как основную анонимную валюту для торговли наркотиками, оружием, поддельными документами и другими нелегальными товарами [5].

DAO (децентрализованные автономные организации) могут быть использованы для организации преступных организаций и группировок, так как они позволяют членам групп анонимно взаимодействовать. DAO могут использоваться для анонимного финансирования криминальных операций, таких как киберпреступность или организация преступных кампаний.

NFT (невзаимозаменяемые токены) используются для отмыwania денег путем спекулятивного повышения цен на цифровые активы, которые являются предметами культуры. Преступники покупают NFT за криптовалюту, полученную преступным путем, а затем продают их по завышенной цене, тем самым легализуя доходы [2]. NFT могут использоваться в схемах по уклонению от налогов, так как они позволяют скрывать активы и переводить средства через границы без контроля со стороны налоговых органов и государства, так как такие операции производятся децентрализованно.

В июле 1989 г. во Франции была создана «группа разработки финансовых мер борьбы с отмыwанием денег», которая является на данный момент международной организацией, именно она разработала перечень рекомендаций по регулированию криптовалют и борьбе с их использованием в преступных целях [3]. ЕС, США и Россия также принимают меры по регулированию криптовалют и борьбе с криптовалютными преступлениями, при этом основываясь на положения, выделенных данной международной организацией. Компании, такие как Chainalysis и CipherTrace, являются передовыми разработчиками инструментов для отслеживания незаконных транзакций с использованием технологий блокчейн и идентификации непосредственных участников транзакций. Многие страны мира ввели юридическую ответственность по преступлениям, которые были совершены с использованием блокчейн-системы и криптовалют. Развитие нормативного регулирования криптовалют и блокчейн системы может способствовать снижению уровня преступной активности, однако может и ограничить разработки в этой области.

Блокчейн является одним из детерминантов преступности, предоставляя преступникам инструменты и условия для сокрытия осуществления факта преступных транзакций. В то же время блокчейн также может быть использован для

борьбы с преступностью, предоставляя инструменты для создания инноваций в сфере отслеживания незаконных денежных переводов и идентификации преступников по их цифровому следу.

Минимизация преступного использования блокчейна возможна путем разработки эффективного нормативного регулирования, использования технологических методов отслеживания транзакций и повышения осведомленности общественности о рисках, связанных с криптовалютами

Будущие исследования должны быть направлены на изучение новых способов использования блокчейна в преступных целях, разработку более эффективных методов противодействия и оценку влияния нормативного регулирования на преступную активность.

Список литературы

1. Федотова В. В., Емельянова Б. Г., Типнер Л. М. Понятие блокчейн и возможности его использования.
2. Europol. (2018). Why is blockchain technology attractive to criminals? Publications Office of the European Union.
3. FATF. (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. Financial Action Task Force.
4. Антонопулос А. М. Осваиваем Биткойн: открываем цифровые криптовалюты // O'Reilly Media. 2014.
5. Атцей Н., Бартолетти М., Чимоли Т. Обзор атак на смарт-контракты: уязвимости, инструменты безопасности и формальная верификация // Международная конференция по принципам безопасности и доверия. 2017. С. 164–187.
6. Грачева Е. Ю., Кучеров И. И., Пономаренко А. Н. Криптовалюта как объект преступного посягательства: криминологический анализ и меры противодействия. // Проспект. 2022.
7. Чихрадзе А. М. Система блокчейн: криминалистический аспект // Философия права. СПб. : 2024.

Корнева Ю. Ю.¹,
старший преподаватель кафедры
административной деятельности ОВД
Московского университета
МВД России имени В.Я. Кикотя,
кандидат психологических наук

ПСИХОЛОГИЯ НЕСОВЕРШЕННОЛЕТНИХ В УСЛОВИЯХ ЦИФРОВОЙ СРЕДЫ: РИСКИ ВОВЛЕЧЕНИЯ В ИТТ-ПРЕСТУПЛЕНИЯ И ВИКТИМИЗАЦИЯ

В настоящее время в период активной информатизации общества одной из приоритетных задач, стоящих перед правоохранительными органами и государством в целом, являются исследования влияния цифровой среды на преступность, возможные риски вовлечения граждан в преступления в сфере ИТ-технологий, а также детерминанты таких преступлений и уровень виктимности. Согласно информации, приведенной главным информационно-аналитическим центром МВД России [7] за прошедший 2024 г., в России киберпреступники все чаще привлекают к совершению правонарушений подростков в возрасте от 14 до 17 лет.

Действительно, несовершеннолетние граждане наиболее подвержены вовлечению в подобного рода преступления. Обусловлено это тем, что данная возрастная категория проводит наибольшее количество времени используя гаджеты и все достижения информатизации в полном объеме. Интернет и онлайн-сервисы предоставляют современным детям широкие возможности и ресурсы для развития, обучения и коммуникации. На сегодняшний день основной психологической проблемой, способствующей активному вовлечению несовершеннолетних в преступную деятельность в сфере ИТ-преступлений, является колоссальный поток информации, поступающей из сети, который невозможно в полной мере контролировать и фильтровать. Наряду с тем немаловажным фактором являются макросоциальные факторы агрессии у подростков. По данным исследований, несовершеннолетние в возрасте от 8 до 18 лет наблюдают на мониторах используемой техники около 10 тыс. актов насилия в год. В результате этого формируются негативные социальные последствия, связанные с психическим здоровьем детей, а также легитимизацией агрессии.

Говоря о виктимизации несовершеннолетних, необходимо выделить несколько факторов ее усиливающих, к таким факторам относятся:

1. Возрастная незрелость – недостаточное количество опыта и знаний, а также чрезмерное любопытство, обусловленное возрастом, внушаемость и склонность к доверчивости.
2. Недостаточная, в силу возраста, осведомленность о безопасном общении посредством сети Интернет и правильных действиях при возможных рисках вовлечения в совершение преступлений.

¹ © Корнева Ю. Ю., 2025.

3. Дефицит позитивного общения в социальной микросреде – зачастую подростки сталкиваются с мнимым недопониманием и обесцениванием их проблем со стороны более взрослого поколения и даже родителей, именно по этой причине им становится намного проще общаться в «онлайн», порой даже с незнакомыми и малознакомыми людьми. При этом сильно возрастает риск быть вовлеченным в правонарушения и надежды несовершеннолетних остаться безнаказанными.

4. Повышенный интерес к негативному контенту – увлеченность запрещенными сайтами, движениями и публикациями в социальных сетях, а также контентом, связанным с рискованным поведением.

Все перечисленные факторы и активное постоянное пользование современных технологий являются благоприятной средой для вовлечения несовершеннолетних в ИТ-преступления. Так, наиболее распространенными преступлениями, совершаемыми несовершеннолетними с использованием ИТТ, являются преступления в сфере хищения чужого имущества. За последние четыре года, по данным официальной статистики МВД России, в 74 раза возросло число преступлений, совершенных лицами не достигшим 18 лет. Такая негативная статистика, как уже было упомянуто, обусловлена в первую очередь психологическими особенностями несовершеннолетних, которые включают в себя влияние отрицательных факторов внешней среды и личности самого несовершеннолетнего на совершение им правонарушений. Безусловно, одними из основных причин индивидуального преступного поведения являются внутренние мотивы, связанные прежде всего со стремлением к самоутверждению.

Говоря о рисках вовлечения несовершеннолетних в преступную деятельность такой направленности, не стоит забывать и о личности преступника, который вовлекает несовершеннолетнего лица в совершение таких преступлений. Напомним, что Уголовный кодекс Российской Федерации предусматривает ответственность за вовлечение несовершеннолетних в совершение преступления [3]. Федеральным законом от 28.12.2024 № 514-ФЗ «О внесении изменений в Уголовный кодекс РФ» [4] в ст. 150 введено несколько квалифицирующих признаков: п. «б», ч. 2 ст. 150 предусматривает ответственность за вовлечение несовершеннолетнего лица в преступление с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), п. «в» ч. 3 устанавливает ответственность за то же деяние в отношении лица, не достигшего четырнадцатилетнего возраста. Таким образом, в совершение преступления несовершеннолетним с использованием ИТ-технологий присутствует сразу два субъекта. С одной стороны, это сам несовершеннолетний, совершивший противоправное деяние, с другой, это лицо, вовлекшее его в преступную деятельность посредством информационных сетей.

Прежде чем привлечь к участию в преступной деятельности тщательно изучается личность, если не каждого несовершеннолетнего индивидуально, то целевой аудитории, на которую направлена агитация и склонение к совершению противоправных деяний. Ведь при этом преступник ищет именно подростков со сложной судьбой или не устойчивой психикой, для. Поэтому, изучая риски участия несовершеннолетних граждан в ИТ-преступлениях, стоит говорить

не только о психофизиологическом состоянии самих несовершеннолетних, но и тех, кто склоняет их к данному роду преступлений.

Таким образом, при изучении психологии несовершеннолетних в условиях глобальной информатизации общества можно сделать вывод о пагубном ее воздействии, поскольку в настоящее время положение несовершеннолетних становится все более уязвимым. И из-за латентности преступной деятельности в сфере информационных технологий, контролировать в полном объеме поток поступающей и обрабатываемой информации невозможно. При этом постепенно законотворческий процесс идет по пути обеспечения безопасности несовершеннолетних, использующих интернет-ресурсы. В настоящее время необходима разработка комплекса мероприятий, направленных на недопущение и профилактику рисков вовлечения несовершеннолетних в преступления в ИТ-сфере, а также снижения уровня виктимности. Правоохранительным органам также стоит координировать свою деятельность для наиболее тесной работы с провайдерами и операторами сетей, это необходимо ввиду специфики цифровых технологий, позволяющих преступнику действовать анонимно. Также стоит привлекать к профилактической работе не только сотрудников правоохранительных органов, но и опытных психологов, специализирующихся на консультировании несовершеннолетних, при этом также не стоит забывать о работе с семьями несовершеннолетних для наиболее тщательного контроля.

Список литературы

1. Конституция Российской Федерации // URL: https://www.consultant.ru/document/cons_doc_LAW_28399/.
2. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» // URL: https://www.consultant.ru/document/cons_doc_LAW_110165/.
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // URL: https://www.consultant.ru/document/cons_doc_LAW_10699/.
4. Федеральным закон от 28.12.2024 № 514-ФЗ «О внесении изменений в Уголовный кодекс РФ» // URL: <https://www.zakonrf.info/doc-38625527/>.
5. Клейберг Ю. А. Психология девиантного поведения // URL: <https://urait.ru/book/psihologiya-deviantnogo-povedeniya-559774>.
6. Криминологическое и уголовно-правовое учение о потерпевшем от преступления // URL: <https://www.litres.ru/book/e-e-popova/kriminologicheskoe-i-ugolovno-pravovoe-uchenie-o-poterpevshem-o-31188839/chitat-onlayn/>.
7. Портал правовой статистики РФ // URL: <http://crimestat.ru/>.
8. Официальный сайт МВД России // URL: <https://мвд.рф/>.
9. Информационное право : учебное пособие / [В. В. Пушкарев, А. В. Константинов, В. Б. Вехов и др.]. М. : Ай Пи Ар Медиа, 2025.
10. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. М. : Ай Пи Ар Медиа, 2025.
11. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов : М. : Профобразование, Ай Пи Ар Медиа, 2025.

12. Константинов А. В. Особенности осуществления деятельности подразделений по делам несовершеннолетних в условиях режима самоизоляции // Портрет инспектора по делам несовершеннолетних : сборник научных трудов Всероссийской конференции, Москва, 28 мая 2020 года. М. : Московский университет МВД России имени В.Я. Кикотя, 2020. С. 239–240.

Кубасов И. А.¹,
профессор кафедры информационных технологий
Академии управления МВД России,
доктор технических наук, доцент

АНАЛИЗ МЕЖДУНАРОДНОГО ОПЫТА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

Киберпреступность является одной из наиболее актуальных проблем современности, представляющей угрозу для экономики, национальной безопасности и стабильности государства. В последние десятилетия наблюдается стремительный рост числа кибератак, затрагивающих государственные институты, коммерческие организации и частных лиц. Правоохранительные органы различных стран предпринимают активные меры по противодействию этому современному феномену [1–3].

В настоящей статье проведен анализ опыта нескольких ведущих стран в области противодействия киберпреступности, рассмотрены основные тенденции и практики, используемые для предотвращения и реагирования на киберинциденты, а также предложены рекомендации по совершенствованию действующих механизмов.

1. Анализ национальных стратегий, законодательных актов, инициатив частного сектора для выявления сходства и различий в подходах государств к решению проблемы противодействия киберпреступности.

Для ведущих стран мира одним из ключевых элементов противодействия киберпреступности выступают законодательные акты, устанавливающие правила и санкции за нарушения в киберпространстве [4]. Вот несколько примеров.

США: В Соединенных Штатах действует обширное законодательство, направленное против киберпреступности, начиная с Закона о компьютерном мошенничестве и злоупотреблении (Computer Fraud and Abuse Act), принятого еще в 1986 г. Особое внимание уделяется защите критической инфраструктуры и вопросам национальной безопасности.

Великобритания: Британское правительство приняло закон Data Protection Act 2018, который гармонизирует британские законы с европейским Регламентом GDPR. Этот акт предусматривает строгие нормы по защите данных и штрафные санкции за нарушения.

Германия: Немецкое законодательство включает Закон о защите данных (Datenschutzgesetz) и Закон о кибербезопасности (IT-Sicherheitsgesetz). При этом уделяется огромное внимание сотрудничеству с частным сектором и академическим сообществом в вопросах кибербезопасности.

Китай: Китай известен своим жестким контролем над интернет-пространством. Государственное регулирование осуществляется через многочисленные законы, такие как Cybersecurity Law of the People's Republic of China, который вступил в силу

¹ © Кубасов И. А., 2025.

в 2017 г. Этот закон устанавливает обязательные требования к компаниям по защите данных и взаимодействию с государственными органами.

Россия: Российская Федерация располагает развитым законодательством в области обеспечения кибербезопасности. Ключевыми документами являются Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон от 26.01.2007 № 152-ФЗ «О персональных данных», Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Эти документы устанавливают общие принципы и требования к защите информации, а также определяют полномочия государственных органов в области кибербезопасности.

2. Анализ организационных структур различных государств по противодействию киберпреступности.

Эффективное противодействие киберпреступности требует наличия компетентных специализированных организаций, занимающихся расследованием и профилактикой киберинцидентов. Вот несколько примеров.

США: Федеральное бюро расследований (FBI) активно занимается вопросами киберпреступности, сотрудничая с частными компаниями и исследовательскими институтами. Агентство национальной безопасности (NSA) также играет значительную роль в мониторинге и предотвращении кибератак.

Великобритания: Национальное агентство по борьбе с преступностью (NCA) ведет активную борьбу с киберпреступниками, работая в тесном контакте с полицией и разведывательными службами. Также создано Национальное агентство по кибербезопасности (NCSC), ответственное за защиту государственной инфраструктуры.

Германия: В стране функционирует Федеральное ведомство по информационной безопасности (BSI), отвечающее за разработку стандартов кибербезопасности и реагирование на инциденты. BSI тесно сотрудничает с частными компаниями и университетами.

Китай: Центральное киберуправление КНР контролирует национальную политику в области интернета и кибербезопасности. Государственная сеть CNCERT работает над мониторингом и реагированием на угрозы.

Россия: ФСБ России и МВД России играют центральную роль в борьбе с киберпреступностью. Специальные подразделения занимаются расследованием киберинцидентов и координацией действий различных силовых структур. Для координации усилий по противодействию киберпреступности созданы специализированные структуры, такие как Национальный координационный центр по компьютерным инцидентам (НКЦКИ, incident@cert.gov.ru) и Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России). НКЦКИ осуществляет мониторинг и реагирование на киберинциденты, а УБК МВД России проводит расследования и привлекает виновных к ответственности.

3. Анализ технических мер, применяемых государствами по противодействию киберпреступности.

Эффективное противодействие киберпреступности невозможно без внедрения современных технологий [5]. Рассмотрим несколько примеров.

США: Американские компании, такие как Microsoft и Google, активно развивают собственные системы кибербезопасности, включая антивирусные программы, фаерволы и облачные сервисы. Правительство инвестирует в проекты по разработке защищенного программного обеспечения и внедрению стандартов шифрования.

Великобритания: Великобритания известна своими проектами по разработке квантовых компьютеров и криптографических протоколов. NCSC активно участвует в тестировании новых технологий и консультировании бизнеса по вопросам обеспечения кибербезопасности.

Германия: Немецкий рынок кибербезопасности выделяется сильными позициями компаний в области промышленного интернета вещей (IIoT) и защиты критической инфраструктуры. Германская промышленность активно внедряет решения по защите промышленных систем управления (ICS).

Китай: Китайская индустрия кибербезопасности развивается в направлении создания собственных аппаратных и программных решений. Страна также инвестирует в исследования в области квантового шифрования и искусственного интеллекта для нужд кибербезопасности.

Россия: Россия активно развивает отечественную продукцию в области обеспечения кибербезопасности, в том числе и антивирусы. Внимание уделяется импортозамещению и локализации технологий, а также защите критической инфраструктуры, включая энергетику, транспорт и финансовые учреждения. Разработаны и внедряются системы обнаружения и предотвращения кибератак, такие как ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак).

4. Анализ состояния международного сотрудничества по противодействию киберпреступности.

Эффективная борьба с киберпреступностью невозможна без международного сотрудничества [6, 7]. Вот некоторые примеры совместных усилий.

Интерпол: Организация объединяет усилия правоохранительных органов различных стран в области противодействия киберпреступности. Специализированные подразделения Интерпола занимаются расследованием транснациональных киберпреступлений.

ООН: Под эгидой ООН проводятся конференции и семинары, посвященные проблемам кибербезопасности. Документ «UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security» предлагает рекомендации по международному сотрудничеству в области кибербезопасности.

Евросоюз: ЕС принимает общеевропейские директивы, направленные на гармонизацию законодательства и создание общей политики обеспечения кибербезопасности. Программа «Digital Single Market» предполагает укрепление киберзащиты в масштабах всего Союза.

Россия активно участвует в международном сотрудничестве по вопросам обеспечения кибербезопасности. Это проявляется в участии в деятельности Интерпола, ОБСЕ и других международных организаций. Россия также заключает двусторонние соглашения с другими государствами для обмена информацией и проведения совместных операций против киберпреступников.

Анализ показывает, что российская система противодействия киберпреступности демонстрирует положительные результаты. Количество раскрытых киберпреступлений увеличивается, а уровень защищенности критической инфраструктуры повышается.

Российский опыт противодействия киберпреступности характеризуется комплексным подходом, сочетающим правовые, организационные и технические меры. Несмотря на достигнутые успехи, необходимо дальнейшее совершенствование системы обеспечения кибербезопасности, включая повышение квалификации специалистов и улучшение информированности граждан. Реализация указанных рекомендаций позволит России оставаться на переднем крае борьбы с киберпреступностью и укрепит ее позиции в международном сообществе.

Следует отметить, что на основе анализа статистических данных о киберпреступности в различных странах мира можно построить следующую модель, отражающую динамику количества киберпреступлений (P) в зависимости от времени (t):

$$P(t) = a \cdot t^2 + b \cdot t + c,$$

где a , b и c — коэффициенты, определяемые эмпирически для каждой страны [8].

Полученная модель убедительно демонстрирует то, что количество киберпреступлений растет нелинейно во времени, что свидетельствует об актуальности дальнейшего наращивания усилий по противодействию киберпреступности.

Таким образом, анализ опыта различных стран показывает, что эффективная борьба с киберпреступностью требует комплексного подхода, включающего законодательные меры, организационные реформы и техническое оснащение. Важно продолжать развивать международное сотрудничество, унифицировать стандарты обеспечения кибербезопасности, совершенствовать законодательство и инвестировать в человеческий капитал. Только объединив усилия, мир сможет успешно противостоять нарастающей угрозе киберпреступности.

Список литературы

1. Тимофеев А. В., Комолов А. А. Киберпреступность как социальная угроза и объект правового регулирования // Вестник Московского государственного областного университета. Серия: Философские науки. 2021. № 1. С. 95–101.
2. Григорьева А. Е. Тенденции и опыт противодействия киберпреступности в России и в зарубежных странах // Аграрное и земельное право. 2024. № 12 (240). С. 441–443.
2. Образцова К. В. Современное состояние борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий и международный опыт противодействия преступлениям в указанной сфере // Актуальные вопросы теории и практики в деятельности подразделений полиции :

Материалы внутриведомственной научно-практической конференции, Волгоград, 30–31 марта 2022 г. М. : Спутник+, 2022. С. 94–101.

3. Основы кибербезопасности : учебник / А. В. Бецков, Б. А. Торопов, В. А. Апульцин [и др.]. М. : Академия управления МВД России, 2023.

4. Самоделкин А. С., Тимофеев С. В. Современные методы выявления и раскрытия преступлений, совершаемых с использованием цифровых технологий // Вестник Восточно-Сибирского института МВД России. 2022. № 2 (101). С. 206–215.

5. Лепешкина О. И. Международное сотрудничество государств СНГ по противодействию киберпреступности // Евразийская интеграция: экономика, право, политика. 2023. Т. 17. № 4 (46). С. 82–91.

6. Карагодин В. Н. Возможности международного сотрудничества при проведении научных исследований транснациональной киберпреступности // Проблемы правовой и технической защиты информации. 2024. № 12. С. 25–30.

7. Актуальные проблемы противодействия преступности : сборник научных трудов. Волгоград : Волгоградская академия МВД России, 2024.

*Лакомская М. Ю.¹,
старший преподаватель кафедры криминалистики
Краснодарского университета МВД России,
кандидат юридических наук*

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ: ВОЗМОЖНОСТИ И НЕДОСТАТКИ

Современный век характеризуется тенденцией активного развития информационных технологий. На данный момент сложно представить какую-либо сферу, которая обходится без внедрения технологический или информационных инноваций. Данная особенность обусловлена упрощением благодаря их использованию многих рутинных, ежедневных задач. И, безусловно, стоит отметить такой скачок, в обозначенной сфере, как искусственный интеллект.

Искусственный интеллект представляет из себя сферу в области компьютерного направления, которая основана на обработке большого объема данных и последующего их анализа, итогом деятельности которого является выявление закономерностей обрабатываемой информации и выполнением поставленных задач.

Искусственный интеллект имеет тенденцию скачкообразного развития. Только в 2020 г. с помощью него создавались хоть и детализированные, но в некотором роде несуразные фото-изображения, и вот на настоящий момент он способен генерировать целые видео и даже имитировать голос человека. Данная особенность вызывает некоторую настороженность, так как невозможно предсказать в каком направлении может и будет развиваться данная технология, поскольку в нее заложено программным путем функции самообучения и какие возможности в себе откроет новое программное обеспечение в виде искусственного интеллекта и как это будет использовано – неизвестно

Искусственный интеллект нашел свое применение и в преступной сфере. Развитие информационных технологий обуславливает новые тенденции совершения преступлений. Только в данной сфере количество зафиксированных преступлений в 2024 г. составляет 577 тыс. Данную информацию изложил начальник Следственного департамента МВД России Даниил Филиппов [4]. Искусственный интеллект является новой веткой развития в преступной сфере, позволяя мошенникам разговаривать голосами родственников выбранной жертвы, заставляя перечислять денежные суммы на свои счета, также создаются новые вредоносные программы, имеющие возможность адаптирования и маскировки от антивирусов индивидуально у каждого компьютера и многое другое.

Но правоохранительные органы также не стоят на месте. Необходимо двигаться в ногу со временем и соответствовать новым предъявленным стандартам. Поэтому искусственный интеллект находит свое отражение и на стороне защитников закона. В своей работе «Искусственный интеллект в криминалистике: состояние и перспективы использования» Д. В. Бахтеев отмечал: «Криминалистика

¹ © Лакомская М. Ю., 2025.

всегда отличалась высокой восприимчивостью к технологиям, потенциально полезным в выявлении и раскрытии преступлений». Данное высказывание небезосновательно, поскольку искусственный интеллект является комплексной и многосторонней программой, так как объединяет в себе два лучших качества сторон человека и машины, а именно когнитивно-мыслительно составляющую и техническую скорость обработки и анализа данных соответственно [1, с. 104].

Таким образом, внедрение в искусственного интеллекта в деятельность лиц, осуществляющих расследование по уголовному делу, преступлений обуславливается следующими факторами [2, с. 47]:

1. Ускорение рутинных, повседневных задач в правоохранительной деятельности.
2. Криминальный интерес и развитие преступной деятельности в данном направлении.
3. Совмещение когнитивных способностей человека и вычислительной мощности техники.
4. Восприимчивость криминалистики к внедрению современных технологий.

Данное направление имело начало еще в 2012 г., когда была создана программа «ФОРВЕР-следователь». Данная программа работает на принципе анализа заранее введенных исходных данных, которые позволяют реализовать на практике понятие криминалистическая характеристика преступлений, а именно создание и расчет условных вероятностей признаков преступления на месте происшествия. То есть, исходя из ранее введенной базы данных, программа сопоставляет новые входные. Далее создаются корреляционные связи, основанные на анализе следов преступления и сопоставляя с ранее совершенными преступлениями выводит следственные версии и план проведения следственных действий, которые основывается на положительном результате в аналогичных ситуациях ранее совершенных преступлений [3, с. 52].

Также стоит отметить систему «Спрут», которая способствует в установлении контактных связей преступников. Исходная база данных позволяет систематизировать все лица входящих в преступные группы или имеющих какие-либо опосредованные связи с преступниками. Внедрение искусственного интеллекта позволит на основе этой базы данных в совокупности с новыми введенными данными о лицах, совершивших преступления, выявить возможные связи с лицами, ранее совершавших преступления, выявить закономерности и иные признаки причастности лиц к преступлениям.

Также не стоит забывать о преступлениях прошлых лет, нераскрытых преступлениях. Создав базу данных об этих преступлениях, возможно на основе недавно полученных сведений о совершенных преступлениях в качестве профилактики вводить их в данную программу. Возможно, вновь совершенные преступления имеют схожий способ совершения или иные следы, что позволит сопоставить данные и способствовать расследованию и раскрытию преступлений.

Эвристические способности искусственного интеллекта к адаптации введенных данных на основе исходных баз данных позволяет крайне эффективно и быстро обрабатывать информацию, полученную в ходе проведения следствен-

ных действий и вырабатывать план для последующих путем анализа аналогичных преступлений, что значительно повышает эффективность деятельности следователя при расследовании преступлений.

Но следует не забывать о индивидуальности подхода к расследованию каждого преступления. Искусственный интеллект основывается на исходных базах данных, безусловно, возможность адаптации и интеллектуального анализа данных позволяет так или иначе открывать некоторые новые возможности при выдвижении следственных версий, выработке плана следственных действий или выявлении закономерностей, но как свойственно и человеку, данная эвристическая способность искусственного интеллекта, нейронных сетей также не исключает ошибок. Как отмечалось ранее, данные программы совмещают лучшие качества человека и машины, но и недостатки также не исключены. В процессе работы, как и человек, получая все более объемную базу данных, исходных сведений, искусственный интеллект будет обучаться и адаптироваться, но для этого нужно время, что способствует уменьшению ошибок, вплоть до полного их отсутствия в некоторых направлениях, но однозначно не во всех.

Именно поэтому роль следователя в расследовании преступлений, а также других сотрудников остается неизменно ведущей, искусственный интеллект остается на данном этапе в роли средства, используемом для повышения эффективности работы следователя и имеет высокий потенциал в будущем, но непредсказуемость развития данного направления, скачкообразность, а также различные факторы, препятствующие расследованию каждого преступления не позволяют стать искусственному интеллекту во главе расследования или иметь статус доказательственной базы при выявлении каких-либо значимых сведений для расследования преступлений.

Список литературы

1. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2 (104).
2. Лебедев М. Д., Саввоев С. А. Использование искусственного интеллекта в расследовании преступлений // Скиф. 2020. № 7 (47).
3. Марфицин П. Г. Компьютерная программа как инструмент формирования и реализации усмотрения следователя // Приволжский научный вестник. 2015. № 12-2 (52).
4. Ущерб от IT-преступлений в 2024 году составил 99 млрд рублей // URL: <https://journal.sovcombank.ru/news/uscherb-ot-it-prestuplenii-v-2024-godu-sostavil-99-mlrd-rublei?ysclid=m2nfr2wgd327143330>&clckid=dd9e5278.

*Мамий А. Х.¹,
преподаватель кафедры уголовного процесса
Краснодарского университета МВД России*

ИДЕНТИФИКАЦИЯ И УСТРАНЕНИЕ ПРЕДВЗЯТОСТИ В ПРОФИЛИРОВАНИИ ПОДОЗРЕВАЕМЫХ В КИБЕРПРЕСТУПЛЕНИЯХ

В эпоху стремительного развития цифровых технологий и неуклонного роста киберпреступности, эффективное выявление и преследование преступников, действующих в онлайн-среде, становится одной из ключевых задач правоохранительных органов. Профилирование подозреваемых в киберпреступлениях, основанное на анализе данных и выявлении характерных признаков, представляется перспективным инструментом в борьбе с этой угрозой. Однако, широкое применение методов профилирования сопряжено с риском предвзятости, обусловленной как несовершенством алгоритмов, так и субъективным восприятием информации сотрудниками правоохранительных органов. Необоснованное включение в профиль отдельных признаков или категорий лиц может привести к дискриминации и нарушению прав граждан, что вступает в противоречие с принципами правового государства.

В этой связи особую актуальность приобретают вопросы идентификации и устранения предвзятости в профилировании подозреваемых в киберпреступлениях. В рамках данного исследования будет рассмотрена проблема предвзятости в контексте применения института преюдиции, а также предложены подходы к совершенствованию существующих методик профилирования, направленные на обеспечение справедливости и объективности при выявлении и преследовании киберпреступников.

Для предварительного следствия ключевое значение имеет поиск и установление доказательств, что продиктовано целями следствия и принципами правового государства. Следовательно, стремясь установить обстоятельства дела согласно ст. 73 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ). Это значит, что все доказательства вины должны быть получены в соответствии с федеральным законодательством, как указано в ст. 50 Конституции РФ и ст.ст. 7 и 75 УПК РФ. В противном случае, даже при наличии сведений о виновности, доказательства будут считаться недействительными.

Законодатель осознает, что процессуальная работа следователя требует времени и внимания к деталям, особенно при составлении протоколов и других документов, влияющих на качество расследования. Институт преюдиции, закрепленный в статье 90 УПК РФ, призван облегчить работу следователей. Важно отметить, что преюдиция не только упрощает работу следствия, но и подчеркивает авторитет судебной власти, выступая в роли законного основания в уголовном процессе.

¹ © Мамий А. Х., 2025.

В соответствии со ст. 90 УПК РФ преюдиция означает, что не требуют дополнительной проверки те обстоятельства, которые установлены вступившим в законную силу приговором в рамках гражданского, арбитражного или административного судопроизводства, но с условием, что «такие приговор или решение не могут предрешать виновность лиц, не участвовавших ранее в рассматриваемом уголовном деле». То есть если суд установил определенные обстоятельства, имеющие в рамках конкретного уголовного дела существенное значение для установления истины, то они могут быть применены «судом, прокурором, следователем, дознавателем» в отсутствие необходимости проведения дополнительных проверочных мероприятий.

Преюдиция аккумулирует в себя некоторые признаки доказательств, которые имеют не только предустановленный характер, но и отчасти снимают со следователя обязанность по дополнительной проверке тех фактов, правовое значение которых определено судом.

Основные условия реализации преюдиции в уголовном процессе:

1. Обстоятельства должны быть установлены судом.
2. Обстоятельства не требуют дополнительной проверки, если имеется вступившее в законную силу решение суда.
3. Обстоятельства должны быть установлены в рамках гражданского, арбитражного или административного процесса.
4. Обстоятельства не могут быть использованы без проведения дополнительной проверки в случае, если приговор постановлен судом в порядке, определенном ст.ст. 226.9, 316 или 317.7 УПК РФ.
5. Обстоятельства, указанные в приговорах, не предрешают виновность лиц, которые ранее не участвовали ранее в рассматриваемом уголовном деле.

При соблюдении указанных условий институт преюдиции может быть использован следователем для установления наиболее значимых фактов по уголовному делу. Однако в данном случае есть несколько аспектов, требующих дополнительного пояснения.

Преюдициальное значение обстоятельств выступает в качестве дополнительного средства формирования доказательственной базы в целях выполнения требований, указанных в ст. 73 УПК РФ, а также для поиска иной информации, имеющей значение для наиболее правильного разрешения дела в рамках правового поля.

По своей юридической природе преюдиция не эквивалента процедуре, связанной с поиском доказательств и установлением обстоятельств совершения преступления, поскольку это бы в значительной степени ограничивало функции института предварительного следствия.

При проведении предварительного следствия стоит понимать, что преюдициальные значения не могут иметь не только те обстоятельства, которые свидетельствуют о виновности лица, который ранее не привлекался по данному уголовному делу, но и те, которые «отражены в оправдательном приговоре, но ставят под сомнение невиновность лица, оправданного по этому же уголовному делу» [5]. То есть при применении установленных судов фактов следователю необхо-

димо помнить про незыблемость презумпции невиновности как конституционного принципа (ст. 49 Конституции РФ), обеспечивающего объективность и всесторонность расследования для последующего принятия решения судом.

Принятые судом решения, вступившие в законную силу, могут быть в установленном законом порядке пересмотрены. По этой причине, когда следователь ссылается на конкретное решение суда по определенному вопросу, он должен иметь в виду, что данное решение может быть пересмотрено или уже пересмотрено. Это таким образом может устранить «предустановленность» фактов и требует их дополнительной проверки, но уже в рамках предварительного следствия.

В рамках предварительного следствия следователям при необходимости апелляции к решениям суда следует обращать внимание исключительно на те решения, которые определяют правовой статус лица. То есть не каждое решение суда можно использовать для установления обстоятельства, имеющих преюдициальное значение. В связи с этим, например, решение, принятое судом об определении стоимости имущества в соответствии со ст. 205 Гражданско-процессуального кодекса Российской Федерации, не может использоваться следователем в качестве обязательного источника для установления сведений, имеющих преюдициальное значение.

Таким образом, институт преюдиции в уголовном процессе имеет важное значение на стадии предварительного расследования, поскольку позволяет экономить временной ресурс следователя и минимизировать производство следственных и иных процессуальных действий в целях установления обстоятельств, имеющих значение для уголовного дела. Тем не менее несмотря на то, что наличие преюдиции в уголовном процессе подчеркивает юридическую силу решений, принятых судом, оно не может заменять собой необходимость производства предварительного следствия и установления вины лица, совершившего преступление, поскольку выступает в качестве факультативного источника установления обстоятельств, предусмотренных ст. 73 УПК РФ [9,10].

Список литературы

1. Тарбагаева Е. Б. Истинность, преюдициальность и законная сила судебного решений // Проблемы доказывания по уголовным делам: межвуз. сб. науч. тр. Красноярск, 1988.
2. Чащина И. В. Преюдиции в уголовном процессе: понятие и значение / И. В. Чащина // Вестник Академии Генеральной прокуратуры Российской Федерации. 2009. № 5 (13). С. 64–67.
3. Суюнова Д. Ж. Особенности института преюдиции в уголовном процессе / Д. Ж. Суюнова // Актуальные научные исследования в современном мире. 2021. № 1-9 (69). С. 289–292.
4. Дядькин О. Н. К вопросу об административной преюдиции // Право и практика. 2022. № 2. С. 65–70.
5. Гриненко А. В. Уголовно-процессуальный кодекс Российской Федерации: постатейный научно-практический комментарий : учебное пособие. 2-е изд., перераб. и доп. М/ : Проспект, 2020.

6. Павлова Ю. В. Легализация (легальное статуирование) судебного акта как юридического факта // Труды Института государства и права Российской академии наук. 2021. Т. 16. № 6. С. 140–165.

7. Авдеев В. Н. Некоторые аспекты реализации института реабилитации в уголовном судопроизводстве России / В. Н. Авдеев, О. А. Ветрова // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 3 (100). С. 126–132.

8. Терентьев А. В. Роль и полномочия суда в уголовном процессе // Юридическая наука. 2024. № 1. С. 67–70.

9. Зинченко М. С. Обстоятельства, подлежащие доказыванию по делам о должностных преступлениях, связанных со взяточничеством // Вестник Костромского государственного университета. 2022. Т. 28. № 2. С. 239–246.

10. Соколов Д. С. Компоненты фактического основания, подлежащие доказыванию для принятия решения о государственной защите участников уголовного процесса / Д. С. Соколов, А. Ю. Афанасьев // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. № 4 (56). С. 113–117.

Поликарпова Е. В.¹,
*старший преподаватель кафедры
противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ: ТЕНДЕНЦИИ И ПРОГНОЗЫ

Современная эпоха характеризуется экспоненциальным ростом зависимости всех без исключения аспектов общественной жизни от функционирования глобальных информационно-телекоммуникационных сетей и цифровых технологий. Сеть Интернет, изначально задуманная как среда для обмена информацией, трансформировалась в обширную и многогранную экосистему, в которой осуществляется экономическая деятельность, социальное взаимодействие, государственное управление и предоставление услуг. Эта трансформация, при всей своей прогрессивности, создала беспрецедентные условия для совершения противоправных деяний, в частности, мошенничества – преступления, основанного на обмане или злоупотреблении доверием. Эффективное противодействие данному виду преступности требует не только адекватного правового регулирования и совершенствования правоприменительной практики, но и глубокого научного осмысления самого феномена, его сущности, форм проявления и детерминант развития.

Проблематика расследования преступлений, совершаемых с использованием средств вычислительной техники, начала активно разрабатываться в отечественной криминалистике еще на заре цифровой эры, о чем свидетельствуют фундаментальные труды профессора В. В. Крылова, заложившего основы криминалистической теории расследования данной категории деяний [1]. В его работах уже тогда отмечалась специфика предмета посягательства, особенностей механизма следообразования и необходимости применения специализированных методов и средств при собирании и исследовании доказательств. Однако стремительное развитие технологий, появление новых сервисов и платформ в сети Интернет привели к качественному изменению самой криминальной активности. Мошенничество в сети Интернет перестало быть маргинальным явлением и превратилось в масштабную, высокодоходную и организованную форму преступности, представляющую серьезную угрозу как для индивидуальных пользователей, так и для хозяйствующих субъектов и государства в целом.

Актуальность исследования современных методов мошенничества в сети Интернет обусловлена не только их широким распространением и значительным материальным ущербом, причиняемым потерпевшим, но и исключительной динамикой их трансформации. Криминальный мир демонстрирует поразительную

¹ © Поликарпова Е. В., 2025.

способность к адаптации, оперативно осваивая новейшие технологии и используя их для совершенствования своих преступных схем. Это ставит перед правоохранительными органами и научным сообществом постоянный вызов, требующий непрерывного анализа, выявления новых трендов и прогнозирования будущих форм криминальной активности.

Современные методы мошенничества характеризуются значительным усложнением, повышением степени изощренности и таргетированности. В отличие от массовых, неперсонализированных атак прошлого, сегодняшние мошеннические схемы часто направлены на конкретные группы лиц или даже на отдельных индивидов, что повышает их эффективность. Так, Н. С. Поликарпов в своих работах справедливо отмечает, что мошенничество в сфере компьютерной информации приобрело характер системного явления, охватывающего различные сферы, от финансовой до бытовой, и совершается с использованием все более сложных технических средств и методов социальной инженерии [2].

Одним из наиболее распространенных и постоянно мутирующих методов является *фишинг*, который вышел далеко за рамки примитивных электронных писем с просьбой подтвердить данные. Сегодня *фишинг* осуществляется через различные каналы: электронную почту, мессенджеры, SMS-сообщения (смишинг), телефонные звонки (вишинг). Особую опасность представляет *целевой фишинг* (spear phishing) и «китовый промысел» (whaling), направленные на конкретных лиц или высокопоставленных сотрудников организаций с целью получения доступа к ценной информации или инициирования несанкционированных финансовых операций [8]. Современные фишинговые сообщения отличаются высокой степенью правдоподобия, имитируя официальные коммуникации от банков, государственных органов, крупных компаний, используя знание специфики деятельности жертвы. Использование методов социальной инженерии достигает такого уровня, что потерпевшие добровольно раскрывают конфиденциальную информацию, будучи убежденными в легитимности запроса.

Другим ключевым направлением является использование вредоносного программного обеспечения (далее – ВПО). Если раньше ВПО использовалось преимущественно для получения несанкционированного доступа к компьютерам или кражи данных, то сегодня оно является неотъемлемой частью мошеннических схем. *Банковские трояны* продолжают совершенствоваться, обходя новые защитные механизмы систем онлайн-банкинга. *Программы-вымогатели* (ransomware), особенно в их современных формах с двойным или тройным вымогательством (шифрование данных, угроза публикации украденных данных, DDoS-атаки на ресурсы жертвы), стали серьезной угрозой для корпоративного сектора, включая финансовые учреждения [10]. Распространение ВПО также стало более изощренным, используя уязвимости в программном обеспечении, зараженные веб-сайты, вредоносную рекламу (malvertising) и те же фишинговые рассылки. Сложность расследования таких случаев многократно возрастает из-за использования полиморфного ВПО, затрудняющего его идентификацию антивирусными средствами, и задействования анонимных сетей и криптовалют для получения выкупа.

Социальная инженерия как метод мошенничества в сети «Интернет» заслуживает особого внимания. В отличие от чисто технических атак, социальная инженерия основана на манипулировании психологией человека. Схемы «Business Email Compromise» (BEC), когда мошенники, выдавая себя за руководителя компании или делового партнера, убеждают сотрудника совершить срочный перевод денежных средств, ежегодно наносят ущерб на миллиарды долларов по всему миру. Романтические мошенничества (romance scams), инвестиционные пирамиды, замаскированные под высокодоходные онлайн-проекты, мошенничества, связанные с продажей несуществующих товаров или услуг в интернет-магазинах и на досках объявлений – все эти схемы активно используют методы убеждения, создания ложного чувства срочности, страха или жадности у потенциальной жертвы. Криминалистический анализ таких преступлений требует понимания не только технических аспектов, но и психологических механизмов воздействия на потерпевшего, что подчеркивает междисциплинарный характер проблематики [4].

Помимо перечисленных, активно развиваются и другие виды мошенничества, например, мошенничество с использованием криптовалют, мошенничество в сфере электронной коммерции, мошенничество с использованием новых технологий и т. д.

Анализируя современную типологию, необходимо отметить, что мошеннические схемы редко существуют в чистом виде. Как правило, они представляют собой комплексные, многоэтапные операции, в которых сочетаются различные методы: например, фишинговая рассылка для доставки вредоносного ПО, которое затем используется для кражи данных, необходимых для совершения финансового мошенничества [8]. Эта конвергенция методов значительно усложняет процесс выявления, пресечения и расследования таких преступлений.

Современное мошенничество в сети Интернет невозможно анализировать в отрыве от технологического контекста. Именно развитие информационно-коммуникационных технологий выступает основным драйвером эволюции криминальных методов. Отмечается, что преступность в целом адаптируется к изменениям в социальной и технологической среде, и киберпреступность является наиболее ярким примером такой адаптации [6].

Искусственный интеллект (далее – ИИ) и машинное обучение (далее – МО) становятся все более значимыми факторами. Мошенники используют ИИ для повышения эффективности своих атак. Например, алгоритмы МО могут анализировать огромные объемы данных о потенциальных жертвах из открытых источников (социальные сети, публичные базы данных) для создания высокоперсонализированных и убедительных фишинговых сообщений. ИИ также может применяться для автоматического поиска уязвимостей в информационных системах, генерации полиморфного вредоносного кода, создания реалистичных голосовых подделок (для вишинга) или дипфейков. Если ранее создание убедительного поддельного контента требовало значительных усилий и навыков, то сейчас соответствующие инструменты становятся все более доступными, что снижает порог вхождения в криминальную деятельность [11]. Прогнозируется,

что в ближайшем будущем ИИ будет активно использоваться не только для создания контента, но и для автоматизации всего процесса мошенничества, от поиска жертвы до вывода похищенных средств.

Технологии распределенного реестра (блокчейн) и криптовалюты, несмотря на свой потенциал для легальных финансовых операций, активно используются мошенниками для анонимизации транзакций и затруднения отслеживания похищенных средств. Хотя большинство публичных блокчейнов обеспечивают псевдоанонимность (транзакции видны, но не привязаны напрямую к личности), использование миксеров (coin mixers), анонимных криптовалют (Monero, Zcash) и многоступенчатых переводов через различные юрисдикции делает процесс финансового расследования крайне сложным [9]. Правоохранительным органам по всему миру приходится осваивать новые методы анализа блокчейн-транзакций и активно взаимодействовать с криптовалютными биржами, многие из которых, однако, зарегистрированы в юрисдикциях с низким уровнем регулирования и кооперации.

Облачные вычисления и сервисы (Cloud Computing) предоставляют преступникам масштабируемую и относительно недорогую инфраструктуру для размещения вредоносных ресурсов, организации DDoS-атак, хранения украденных данных. Использование облачных сервисов затрудняет физическое обнаружение криминальной инфраструктуры и требует сложных юридических процедур для получения доступа к данным, хранящимся у провайдеров в других юрисдикциях [4].

Даркнет (Dark Web) и различные инструменты анонимизации (сети TOR, VPN, защищенные мессенджеры) продолжают оставаться ключевыми элементами инфраструктуры киберпреступности. Именно в даркнете происходит торговля украденными данными, вредоносным программным обеспечением, инструментами для взлома, а также осуществляется координация деятельности преступных групп. Анонимность, предоставляемая этими инструментами, является серьезным вызовом для идентификации преступников и сбора доказательств [8].

Важным организационным аспектом является индустриализация киберпреступности. Современное мошенничество в сети Интернет все чаще совершается не одиночками, а высокоорганизованными транснациональными преступными группами. Наблюдается четкая специализация: одни участники занимаются разработкой ВПО, другие – фишинговыми рассылками, третьи – обналачиванием похищенных средств, четвертые – социальной инженерией [8, 10]. Появилась даже модель «Киберпреступность как услуга» (Cybercrime-as-a-Service, CaaS), когда специализированные группы предлагают другим криминальным элементам аренду своей инфраструктуры, ВПО, ботнетов или услуг по отмыванию денег. Эта модель значительно снижает технический порог вхождения в киберпреступность для новых акторов и масштабирует угрозу. Организованный характер и транснациональность киберпреступных групп создают серьезные препятствия для их выявления, пресечения и привлечения к ответственности из-за сложности трансграничного взаимодействия правоохранительных органов [4, 9].

Таким образом, технологический прогресс, активно используемый криминальным миром, в сочетании с высокой степенью организации и специализации

преступных групп, детерминирует беспрецедентный уровень сложности и масштаба современного мошенничества в сети Интернет.

Анализ современных методов мошенничества и технологических детерминант позволяет выявить ряд устойчивых тенденций, определяющих векторы их дальнейшего развития:

1. Увеличение степени технологической изощренности и автоматизации.
2. Конвергенция и гибридизация методов.
3. Рост таргетированных атак.
4. Экспансия в новые цифровые среды.
5. Усиление роли организованной преступности и «CaaS».
6. Использование мошенничества в геополитических целях.

Эти тенденции указывают на то, что угроза интернет-мошенничества будет не только сохраняться, но и качественно меняться, становясь более масштабной, изощренной и трудноискоренимой без принятия адекватных мер противодействия.

Основываясь на выявленных тенденциях, можно сформулировать ряд прогнозов относительно будущих форм интернет-мошенничества и вызовов, с которыми столкнется правоохранительная система:

1. Доминирование ИИ-генерируемого контента в мошеннических схемах.
2. Увеличение сложности финансовых потоков и отмывания денег.
3. Рост атак на новые цифровые активы и среды.
4. Увеличение роли инсайдерских угроз и сговора.
5. Эскалация «гонки вооружений» между мошенниками и защитниками.

Проведенный анализ современных методов мошенничества в сети Интернет свидетельствует о качественной трансформации данного вида преступности, детерминированной стремительным развитием цифровых технологий и адаптивными способностями криминального мира. От примитивных форм, перенесенных из оффлайн-среды, мошенничество эволюционировало до высокотехнологичных, сложноорганизованных и таргетированных операций, активно использующих потенциал искусственного интеллекта, технологий распределенного реестра и облачных вычислений.

Ключевыми тенденциями являются увеличение технологической изощренности и автоматизации атак, конвергенция различных методов, рост таргетированности, экспансия в новые цифровые среды и усиление роли организованной преступности. Эти тенденции обуславливают серьезные вызовы для правоохранительной системы, связанные с юрисдикционными коллизиями, сложностью доказывания в цифровой среде, проблемой атрибуции преступников и отставанием законодательства от технологического прогресса.

Список литературы

1. Крылов В. В. Основы криминалистической теории расследования преступлений, совершаемых с использованием средств вычислительной техники. М. : Проспект, 1998.

2. Поликарпов Н. С. Расследование мошенничества в сфере компьютерной информации. М. : Юрлитинформ, 2017.
3. Сухарев В. Н. Киберпреступность: понятие, виды, криминалистическая характеристика. М. : Юрлитинформ, 2014.
4. Матвеев И. М. Проблемы доказывания по уголовным делам о преступлениях в сфере компьютерной информации. М. : Юрлитинформ, 2019.
5. Россинская Е. Р. Цифровая криминалистика. М. : Проспект, 2021.
6. Wall D. S. *Cybercrime: The Transformation of Crime in the Information Age*. Polity, 2007.
7. Grabosky P. N. *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. Federation Press, 1999.
8. Broadhurst R. G. Developments in the global cybercrime economy. *European Journal of Criminology*, 2006, vol. 3, no. 4, pp. 405–422.
9. Casey M. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed. Academic Press, 2011.
10. Jaishankar K. (Ed.). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press, 2011.
11. Chen T., et al. AI-driven Phishing Attack Generation and Detection. *Journal of Cybersecurity*, 2022, vol. 8, no. 1.
12. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. М. : Ай Пи Ар Медиа, 2025.
13. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. М. : Московский университет МВД России им. В.Я. Кикотя, 2024. С. 35–37.
14. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. 2024. № 5. С. 149–155.
15. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова. М. : Изд-во Юридического института РУТ (МИИТ), 2025.

Попенков А. В.¹,
*старший преподаватель кафедры
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

ПРОТИВОДЕЙСТВИЕ НЕЗАКОННОЙ КОЛЛЕКТОРСКОЙ ДЕЯТЕЛЬНОСТИ В СОВРЕМЕННОМ ЦИФРОВОМ ПРОСТРАНСТВЕ

Возврат задолженностей перед банками и микро финансовыми организациями на сегодняшний день стал обыденной процедурой, которая достаточно регламентирована и понятна, благодаря действующему законодательству, однако все еще остаются вопросы, связанные с незаконными действиями и преступными способами возврата долгов со стороны коллекторских агентств. По состоянию на январь 2025 г., количество официально зарегистрированных коллекторских агентств в России составляло 353 организацию, из которых 314 организаций банки и 39 не банковские организаций. [1] Только за 2023 г. коллекторские агентства получили от банковских организаций долгов физических лиц на 582 млрд рублей, для сравнения суммарная прибыль банка «ВТБ» за аналогичный период составила 432 млрд рублей. [2] Такой оборот денежных средств для указанной сферы колоссален, однако эти деньги нужно еще истребовать с должников, а это вопрос долговременный и не всегда успешный, в связи с чем коллекторские агентства спешат получить доход быстрыми, но не всегда законными методами. Об этом свидетельствует и планомерное ужесточение ответственности, за незаконную деятельность коллекторов по возврату долгов с физических лиц. Так, с принятием Федерального закона от 10.07.2023 № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и ст.ст. 150 и 151 Уголовно-процессуального кодекса Российской Федерации» в УК РФ введена ст. 172.4 «Незаконное осуществление деятельности по возврату просроченной задолженности физических лиц», которая была призвана ликвидировать потребность коллекторов во взыскании денежных средств с должников любыми методами. Государственная регламентация деятельности коллекторских агентств, а также введение уголовной ответственности для лиц, не соблюдающих правовые нормы истребования долгов с физических лиц, не ликвидировала полностью незаконные методы работы агентств, однако послужила стимулом к повышенной осторожности при осуществлении незаконных методов взыскания. Одним из способов обезопасить свою деятельность было смещение направленности в цифровую среду и переход к анонимизации. Мы должны понимать, что коллекторское агентство – это не предприятие с оборудованием, на которое можно наложить арест, в качестве обеспечительной меры, не государственный архив с массивом бумажных документов, подлежащих изъятию, и даже не кри-

¹ © Попенков А. В., 2025.

минальный колл-центр с рабочими местами и фактическим адресом. Коллекторское агентство – это ноутбук с базами данных и программным обеспечением, а также мобильные средства связи и выхода в Интернет. Таким образом, незаконная деятельность может осуществляться без привязки к чему-либо стационарному, вплоть до работы из машины, припаркованной у дома должника. Да, на сегодняшний день коллекторские агентства уходят от классических криминальных схем, сопряженных с откровенным насилием и уничтожением имущества, однако бесконтактный способ оказания давления на должника по-прежнему входит в их инструментарий [3, с. 203–207].

Осуществляя свою противоправную деятельность, коллекторы осознают фактический характер своих действий, их последствия и желаемый к получению результат, таким образом, они, во-первых, всегда готовы к вероятности уголовного преследования, во-вторых, они принимают все меры предосторожности для уклонения от наступления уголовной ответственности, в-третьих/ всегда обеспечены компетентной юридической защитой, осуществляемой на договорной основе через аффилированные с ними адвокатские структуры.

С технической точки зрения анонимайзинг незаконной деятельности коллекторов обеспечивается достижениями современной науки и техники, а именно:

- использование виртуальных СИМ карт для звонков, не привязанных к какому-либо лицу;
- использование серверов VPN, для анонимного доступа в интернет;
- рассылка корреспонденции с фейковых аккаунтов и электронной почты;
- использование программ модуляторов, для видеоизменения голоса, кратно усложняющих проведение фоноскопических экспертиз;
- использование ИИ для генерации фейковых документов и пр.;
- заражение устройств должника вредоносным программным обеспечением.

Таким образом, цифровые следы, оставленные коллекторами часто мало пригодны для криминалистической идентификации и последующего использования в качестве доказательной базы по уголовному делу. Более того, наивно полагать, что электронные сведения о подобных операциях против должников, выходящих за рамки правового поля, не обеспечены средствами защиты, в том числе и функцией самоликвидации, в случае попыток доступа к ним из вне. [4, с. 12–17]

По данным статистики, подавляющее большинство (63 %) коллекторских организаций расположены, зарегистрированы и функционируют в г. Москве, что позволяет органам дознания и предварительного следствия эффективно использовать весь электронный функционал, имеющийся в Московском регионе («Безопасный город», «Парсив», «Магистраль» и т. д.) для установления виновных лиц и привлечения их к уголовной ответственности.

Важным аспектом выявления лиц, причастных к совершению преступления, является продуктивное взаимодействие правоохранительных органов с банковскими структурами. В настоящее время вывод денежных средств также прозрачен и при правильном алгоритме отследить движение денежных средств должника вполне возможно вплоть до конечного получателя.

В свете озвученной выше проблематики следственным органам целесообразно привлекать для оперативного сопровождения и разработки такой преступной деятельности компетентные технические органы МВД России, в том числе БСТМ МВД России, экспертов-криминалистов, специалистов по кибер-преступлениям. Это обусловлено тесной взаимосвязью правоприменительной практики и технических познаний, необходимых для сбора доказательной базы по преступлениям данной категории. Следует учесть, что установление способов совершения преступления с использованием цифровых ресурсов не дает возможности выйти на след исполнителей, а установление исполнителей, без определения средств и способов совершения ими преступления не дает оснований привлечения их к уголовной ответственности. [5, с. 352–353]

Совершенно очевидно, что развитие коллекторской деятельности в России будет иметь продолжение, а использование цифровых ресурсов коллекторскими агентствами продолжится, в результате чего, органам предварительного расследования необходимо уже сегодня принимать меры, по контролю за цифровой средой, для раскрытия уже совершенных преступлений и пресечения преступных деяний в будущем.

Список литературы

1. Коллекторские агентства (рынок России) // Tadviser. URL: <https://www.tadviser.ru/index.php>.
2. ВТБ ждет чистую прибыль в 2024 году ближе к 500 млрд рублей // Интерфакс. URL: <https://www.interfax.ru/business/962423>.
3. Нуйкин С. Ю. Особенности расследования преступлений, совершаемых через интернет-ресурсы / С. Ю. Нуйкин, К. О. Ильинская // Актуальные вопросы производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства : сборник научных трудов Всероссийской научно-практической конференции, Москва, 7 апреля 2022 г. М. : Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. С. 203–207.
4. Лебедева А. А. Использование сети Интернет для раскрытия и расследования преступлений / А. А. Лебедева // Цифровые технологии современной криминалистики, использование специальных знаний : Материалы конференции, проведенной в рамках XXVII Международной выставки средств обеспечения безопасности государства «Интерполитех-2023», Москва, 18 октября 2023 г. М. : Московская академия Следственного комитета Российской Федерации, 2024. С. 12–17.
5. Брылева Т. О. Проблемные вопросы расследования вымогательства посредством применения кибербуллинга / Т. О. Брылева // Правопорядок в России: проблемы совершенствования : Сборник научных трудов XVII Всероссийской научно-практической конференции, Москва, 13–17 февраля 2023 г. М. : Московский университет МВД России имени В.Я. Кикотя, 2023. С. 352–353.

Пучков Г. Ю.¹,
*ведущий научный сотрудник
ФКУ НПО «СТuС» МВД России,
кандидат технических наук*

АНАЛИЗ ВОЗМОЖНЫХ НАПРАВЛЕНИЙ ДАЛЬНЕЙШЕГО РАЗВИТИЯ КРИМИНАЛЬНЫХ ТЕХНОЛОГИЙ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Стремительное развитие искусственного интеллекта (далее – ИИ) в последние годы создало предпосылки для его внедрения практически во все сферы человеческой деятельности – от медицины и финансов до образования и развлечений, в результате чего возможности ИИ представляются безграничными: от автоматизации рутинных задач до создания сложнейших прогнозных моделей и разработки инновационных лекарств. Однако эти же возможности привлекают и злоумышленников, которые все чаще используют ИИ для совершения преступлений в киберпространстве. В условиях растущей зависимости общества от информационных технологий и цифровизации всех аспектов жизни, киберпреступность стала глобальной угрозой, а ИИ выступает как мощное оружие в руках хакеров и мошенников, так как вместе с бурным развитием нейросетевых технологий совершенствуются технологии, способы и методы преступной деятельности [1].

Преступления в сети Интернет с использованием ИИ с каждым годом занимают все более заметное место в структуре всех зарегистрированных преступлений в стране. Если в 2018 г. их удельный вес составлял порядка 9 %, то уже в 2023 г. – почти 35 %. Наибольшее количество таких преступлений (почти 70 %) связано с хищениями собственности.

Учитывая изложенное, вопросы прогнозирования возможных направлений дальнейшего развития криминальных технологий с использованием ИИ весьма актуальны в настоящее время. В этой связи рассмотрим следующие варианты применения ИИ в противоправной деятельности.

Беспилотные транспортные средства. Анализ опыта проведения террористических акций показывает, что беспилотные транспортные средства (БТС) используются обычно в качестве средств доставки взрывчатки. Однако в последнее время наметилась тенденция использования БТС и как самостоятельное кинетическое оружие. Объясняется это тем, что в большинстве стран транспортные средства более доступны, чем огнестрельное оружие и взрывчатка, а теракты с использованием транспортных средств могут быть организованы с меньшими организационными издержками разрозненными, квазиавтономными или «одиночными» террористами, например, членами таких террористических организаций, как ИГИЛ, «братья мусульмане» и т. д.

Эта тактика приобрела особую популярность после серии терактов в западных городах, включая Ниццу (2016), Берлин (2016), Лондон (2017), Барселону

¹ © Пучков Г. Ю., 2025.

(2017) и Нью-Йорк (2017) [2]. В настоящее время полностью автономные беспилотные автомобили, управляемые искусственным интеллектом, преступникам не доступны, ввиду их отсутствия. Однако ведущие производители автомобилей и технологические компании намерены создать такие автомобили в ближайшее время (опытные образцы в настоящее время проходят испытания на дорогах общего пользования).

Появление автономных БТС позволит решить одну из главных проблем террористов – наем водителей для доставки транспортного средства к месту проведения террористического акта. Кроме того, это позволит преступникам совершать несколько нападений одновременно. При этом, используя возможности сети Интернет, сотовых и спутниковых систем по организации глобальной связи, управление данными транспортными средствами можно осуществлять из единого центра, расположенного в безопасном (для террористов) месте, без участия человека (при помощи нейросетевых технологий), что позволит проводить теракты с использованием БТС практически в любой точке планеты.

Учитывая изложенное, можно спрогнозировать, что в обозримой перспективе беспилотные автономные транспортные средства могут стать основой для развития новых способов автотранспортного терроризма.

Индивидуальный фишинг. Фишинг – это атака с использованием «социальной инженерии», цель которой сбор конфиденциальной информации или установка вредоносного программного обеспечения (ПО) с помощью цифрового общения, отправленного якобы доверенным лицом, например, из банка пользователя, с его места работы, от родственников.

Злоумышленник использует доверительные отношения, чтобы убедить пользователя выполнить действия, благодаря которым его персональные данные будут скомпрометированы, например, раскрыть пароли доступа или перейти на специализированные сайты для совершения преступных действий от имени пользователя [3]. В перспективе атаки могут быть двух видов – персональные и масштабные.

Персональные атаки нацелены на конкретных людей. Подготовка данных атак предусматривает тщательное изучение характера, привычек и особенностей поведения жертвы в киберпространстве, с тем чтобы в дальнейшем при помощи современных инструментов ИИ использовать данную информацию для компрометации его персональных данных в основном с целью хищения денежных средств. Это так называемый «персонализированный фишинг». Широко он не используется, так как требует значительных временных затрат на изучение поведения жертвы. Применяется, как правило, в отношении лиц, обладающих значительными финансовыми средствами.

Масштабные фишинговые атаки ориентированы на массовую рассылку фальшивых сообщений, нацеленных на выявление лиц, которые могут быть подвергнуты дальнейшему фишинговому прессингу для получения их персональных данных. Для этого используются шаблонные сообщения, оформленные в стиле известных брендов или актуальных событий, которые могут заинтересовать некоторую часть пользователей чисто случайно [4]. Здесь ставка делается на то, что в результате отправки большого количества цифровых сообщений, удастся

выявить достаточное количество потенциальных жертв, которых можно ввести в заблуждение, не тратя время на использование методов «персонального фишинга».

Анализ темпов и направлений развития искусственного интеллекта, который может быть использован для реализации фишинговых атак, показывает, что уже в 2025 г. их эффективность может быть существенно увеличена за счет применения методов «персонального фишинга» для организации масштабных атак и адаптации данных сообщений путем изменения его деталей в случае неудачных попыток, используя для этого активное обучение применяющихся для подготовки ложных сведений нейросетей при помощи новых инструментов ИИ, т. е. совершенствуя преступный ИИ при помощи последних достижений в области ИИ.

Системы с критической инфраструктурой. Современные достижения в области искусственного интеллекта широко используются в настоящее время для повышения уровня комфорта и удобства граждан. При этом мало кто задумывается о возможных рисках, которые данные действия создают в сфере обеспечения безопасности граждан. Как правило, системы, предназначенные для решения городских бытовых обыденных проблем (управление транспортной сетью, энерго- и водоснабжением, лифтовыми сетями и т. д.) не воспринимаются как критически важная инфраструктура.

Современные тенденции цифровизации коммунальных систем предполагают повсеместное внедрение технологий искусственного интеллекта и нейронных сетей. Это позволяет повысить автоматизацию, адаптивность и эффективность функционирования систем, однако, порождает новые уязвимости в системе их кибербезопасности.

Миграция управления данными системами на платформы, основанные на современных нейронных сетях, открывает новые возможности для преступников и террористов. Переход на ИИ-управление влечет за собой серьезный риск целенаправленного саботажа, последствия которого могут быть катастрофическими.

Масштабные перебои в снабжении электроэнергией, парализующие целые города, огромные транспортные заторы, приводящие к хаосу в результате нарушения процедур поставки продуктов питания и медикаментов, нарушения водоснабжения и работы канализационных систем, вызывающие массовые отравления и эпидемии, это далеко не полный список возможных последствий кибератак на компьютеризованные процедуры управления коммунальными системами с критической инфраструктурой.

Анализ тенденций в области развития технологий взлома и компрометации кибер. систем показывает, что в ближайшее время атаки на системы с критической инфраструктурой, управление которыми осуществляется при помощи нейросетей, будут осуществляться по трем основным направлениям.

Используя уязвимости в программном коде. Нейронные сети, использующиеся для принятия решений в реальном времени, могут содержать ошибки программной реализации, что может быть использовано злоумышленниками. Атаки на программный код или интерфейсы взаимодействия могут привести к нарушению функционирования системы.

Примером является атака на систему энергоснабжения Украины в 2015 г., при которой злоумышленники использовали уязвимости программного обеспечения для дестабилизации работы электросетей [5].

Используя подмену данных на этапе обучения модели. Нейронные сети требуют значительных объемов данных для обучения. Подмена или манипуляция обучающими выборками может привести к появлению скрытых уязвимостей в модели, что открывает возможность для целенаправленного воздействия на системы управления. Данный вид атак особенно опасен в системах с длительными циклами обучения, где контроль качества данных может быть затруднен. Манипуляция данными может осуществляться путем внедрения небольшого количества специально подготовленных ложных данных, которые незаметны на этапе валидации, но в процессе эксплуатации при получении условных команд способны существенно изменить поведение модели.

Применяя атаки с использованием вредоносных данных (data poisoning). Это так называемые «атаки с сопоставлением данных», нацеленные на внесение изменений во входные данные, провоцируя некорректные или разрушительные решения со стороны модели. Эти атаки могут быть реализованы путем внедрения ложных данных в процессе эксплуатации системы.

При этом при подготовке указанных атак ожидается проявление следующих тенденций:

- повышение сложности атак с использованием методов adversarial machine learning;
- применение генеративных нейронных сетей для создания фальсифицированных данных, вводящих модели в заблуждение;
- использование автономных ИИ-агентов в атаках на распределенные системы управления (SCADA);
- применение методов глубокого обучения для автоматической адаптации атакующих стратегий к защитным мерам.

Масштабный шантаж. Традиционный шантаж предполагает вымогательство под угрозой обнародования доказательств преступной деятельности или правонарушений, а также компрометирующей личной информации, при этом ограничивающим фактором является размер вознаграждения – преступление имеет смысл только в том случае, если плата за сокрытие доказательств будет значительно больше, чем затраты на их получение.

В этой связи в ближайшей перспективе следует ожидать бурного развития данного вида преступлений, так как современные, а тем более перспективные инструменты ИИ позволят существенно снизить затраты на получение компрометирующих сведений за счет использования для этого методы аналитического анализа данных находящихся в социальных сетях, архивах электронной почты, браузерах, на жестких дисках компьютеров и в телефонах.

Анализ возможностей современных инструментов ИИ, предназначенных для автоматизированного анализа больших массивов данных, выявления аномалий или потенциально компрометирующей информации показывает, что в ближайшей перспективе для подготовки материалов для шантажа широкое применение найдут генеративные нейронные сети (GAN) [6], которые будут использоваться

для создания фальсифицированных доказательств, трудно отличимых от подлинных. Например, обнаруженная в переписке уязвимая информация может быть дополнена искусственно сгенерированными письмами или изображениями, что делает обвинительные материалы более убедительными и сложными для опровержения.

С развитием ИИ можно прогнозировать дальнейшее усложнение атак. В ближайшие два года ожидаются:

- совершенствование методов автоматизированной генерации компрометирующих материалов, что может привести к созданию более реалистичных поддельных изображений, аудио- и видеозаписей и будет способствовать повышению уровня доверия к фальсифицированным доказательствам;
- активизация целевых атак с использованием профилирования личности: на базе комплексных профилей, составленных на основе анализа поведения в сети, социальных связей и текстовых сообщений, повышая вероятность успешного шантажа;
- области предсказательной аналитики будут созданы более совершенные алгоритмы машинного обучения для прогнозирования реакции жертвы на шантаж, что позволит преступникам выбирать наиболее эффективные тактики давления;
- широкое использование гибридных атак, т. е. различных комбинаций реальных и фальсифицированных данных, что сделает компрометирующие материалы более убедительными и сложными для опровержения.

Вместе с тем необходимо отметить, что несмотря на широкие возможности технологий ИИ для организации противоправных действий, своевременное принятие контрмер позволяет существенно снизить их эффективность. Очевидно, что любая новая киберугроза будет обладать своими специфическими особенностями и требовать на свое отражение действий, которые эту специфику учитывают. Тем не менее комплексное применение основных способов защиты в большинстве случаев позволяет отразить нападение.

Проведенный анализ возможных направлений дальнейшего развития криминальных технологий с использованием искусственного интеллекта показывает, что противодействие преступлениям, связанным с использованием технологий ИИ, требует внедрение в деятельность правоохранительных служб новых можно сказать революционных технологий, подготовки оперативных сотрудников, имеющих высокую квалификацию в сфере ИИ, усиления международного сотрудничества для обмена опытом и координации совместных действий.

В условиях стремительно меняющегося цифрового пространства только комплексный подход позволит обеспечить надежную защиту персональных данных и обеспечить минимизацию последствий преступного использования технологий ИИ.

Список литературы

1. Пучков Г. Ю. Анализ киберугроз, подготовленных с использованием последних достижений в области технологий искусственного интеллекта // Промышленность и сельское хозяйство. 2024. № 10. С. 89–95.
2. URL: <https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8/>.
3. Бодди М. Фишинг 2.0: новая эра киберпреступности // Бюллетень по компьютерному мошенничеству и безопасности. 2018. № 11. С. 8–10.
4. URL: <https://securelist.ru/spam-and-phishing-in-2018/93453/>.
5. Lee R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Working Paper CISL. 2021. С. 1–34.
6. Питерс К. М. Преступление в XXI веке: как вредоносный искусственный интеллект повлияет на национальную безопасность // Искусственный интеллект. Киберпреступность. 2021.

Рудин А. В.¹,
*старший преподаватель кафедры
 противодействия преступлениям в сфере
 информационно-телекоммуникационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат юридических наук*

ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Цифровая трансформация общества достигла стадии, когда она кардинально меняет саму природу преступной деятельности. На этом фоне исследование преступлений, совершаемых с использованием искусственного интеллекта (ИИ), переходит из разряда перспективных в категорию неотложных. По справедливому замечанию В. А. Тирраней, проникновение ИИ-технологий порождает принципиально иные вызовы для уголовно-правовой системы, ставя под сомнение адекватность традиционных доктринальных конструкций [1].

Подтверждением масштаба проблемы служат данные МВД России: в 2024 г. зафиксировано свыше 765 тыс. киберпреступлений, что на 13,1 % выше уровня 2023 г. Более того, анализ этих цифр показывает не только количественный скачок, но и качественную трансформацию: способы совершения преступлений усложняются за счет внедрения самообучающихся алгоритмов, делая угрозы более изощренными и адаптивными.

Правовая доктрина не выработала консенсуса относительно дефиниции искусственного интеллекта (ИИ) в уголовно-правовом поле. Так, проект американского закона «Future of Artificial Intelligence Act» (2017) трактует ИИ узкотехнически – как «искусственные системы», функционирующие в динамичной среде без постоянного человеческого контроля [6]. В противовес этому российские ученые разрабатывают более развернутые дефиниции, подчеркивающие ключевые атрибуты систем: способность к самообучению и адаптации [2].

Данная терминологическая неоднозначность порождает фундаментальную для уголовного права дилемму: является ли ИИ лишь усовершенствованным *инструментом* преступления или его *квазисубъектом*. От решения этого вопроса напрямую зависят основания уголовной ответственности. Некоторые ученые настаивают, что ИИ остается «усложненным» орудием, аналогичным специализированному ПО [4]. Однако в научном дискурсе все громче звучат голоса в пользу придания автономным ИИ-системам особого статуса. Дискуссионная концепция «электронного лица», предполагающая ограниченную правосубъектность для ИИ, служит яркой иллюстрацией этих тенденций [3].

Эмпирические исследования криминального применения ИИ фиксируют тревожную эволюцию: от разрозненных противоправных актов к комплексным,

¹ © Рудин А. В., 2025.

многоуровневым атакам на критическую инфраструктуру. Наглядной демонстрацией уязвимости стал инцидент 2019 года в Японии, где ИИ осуществил серию согласованных кибератак на банковский сектор, приведших к масштабным хищениям. Параллельно экспоненциально усложняется процесс детекции подобных преступлений, особенно с распространением генеративных нейросетей, создающих синтетический медиаконтент, неотличимый от аутентичного даже для специализированного софта.

Эффективное противодействие преступности с применением искусственного интеллекта (ИИ) требует создания их всеобъемлющей типологии. Ключевым критерием классификации выступает объект преступного посягательства:

1. Преступления против собственности: Автоматизированное мошенничество, компрометация платежных систем, управление ботнетами для хищений. (Инструменты ИИ: автономные системы, самообучающиеся алгоритмы; примеры: автоматизированный взлом платежных систем, ботнеты для DDoS, программные роботы для криптоопераций).

2. Преступления против личности: Генерация компрометирующего deepfake-контента, кибербуллинг с применением ИИ, алгоритмическая дискриминация. (Инструменты ИИ: генеративные нейросети, deepfake-технологии; примеры: создание/распространение фальшивого видео/аудио для обмана, кибербуллинг через чат-боты).

3. Преступления против общественной безопасности (наиболее опасные): Атаки на критическую инфраструктуру, масштабные DDoS-атаки, распространение адаптивного вредоносного ПО. (Инструменты ИИ: адаптивные вредоносные программы, централизованные ИИ-системы управления; примеры: кибератаки на энергетику/транспорт, вредоносы для систем госуправления).

Не менее значим технологический критерий, выявляющий инструментарий злоумышленников: генеративные модели (фальсификация контента), самообучающиеся алгоритмы (поиск уязвимостей), автономные системы (атаки без постоянного контроля), адаптивные вредоносы (изменение параметров). Стремительная эволюция ИИ размывает границы между этими категориями, диктуя необходимость постоянного совершенствования криминологических методов и оперативной коррекции правовых механизмов противодействия. Данный контекст подчеркивает критическую важность междисциплинарных исследований, объединяющих юристов, IT-специалистов и криминалистов.

Проблемы юридической квалификации остаются центральными при расследовании ИИ-преступлений. Дискуссионным является вопрос оценки общественной опасности. Как аргументирует В. Г. Беляев, она должна определяться не только реальным ущербом, но и потенциалом масштабирования – один ИИ-бот способен совершить тысячи мошеннических операций, что качественно отличает такие деяния от традиционной киберпреступности [5].

Ключевыми дискуссионными аспектами квалификации являются:

1. Установление субъективной стороны. Как вменять умысел разработчику/оператору, если преступный результат достигнут благодаря самообучению алгоритма? Доктринальные решения варьируются от «предвидимых последствий» до «рискованного замысла».

2. Распределение ответственности. Опыт США (дело *United States v. Vasquez*, 2024) показывает попытки дифференцировать вину между создателями и пользователями ИИ в зависимости от осведомленности о криминальном потенциале [8].

3. Пробелы в законодательстве. Отсутствие в УК РФ специальных норм об ИИ-преступлениях ведет к применению аналогии закона (например, *deepfake*-мошенничество по ст. 159 УК РФ), что неадекватно отражает их повышенную общественную опасность.

Сравнительно-правовой анализ выявляет различные регуляторные модели: Европейский «AI Act» фокусируется на «риск-ориентированном» регулировании для высокорисковых ИИ-систем; китайские «Deep Synthesis Management Regulations» требуют обязательной маркировки синтетического контента [7].

В российской правовой доктрине обсуждаются концепции совершенствования законодательства:

Введение специального квалифицирующего признака «использование ИИ» в соответствующие статьи УК РФ.

Разработка профильного федерального закона об ответственности за разработку и применение ИИ-технологий.

Формирование специализированных подразделений в правоохранительных органах для расследования ИИ-преступлений.

Особого внимания заслуживает инициатива по разработке международной конвенции по борьбе с ИИ-преступностью (по аналогии с Будапештской конвенцией), способной унифицировать криминализацию и создать глобальные механизмы сотрудничества.

В заключение преступления с использованием ИИ представляют собой качественно новый и эволюционирующий феномен современной преступности, характеризующийся исключительной опасностью вследствие способности к масштабированию, адаптивности и сложности выявления. Адекватное противодействие этим вызовам требует глубокой модернизации уголовно-правового регулирования, поиска баланса между защитой общественных интересов и стимулированием инноваций. Перманентное развитие технологий будет неизбежно порождать новые инструменты и формы криминальной активности, что обуславливает необходимость непрерывного обновления классификационных подходов и аналитических методик. Таким образом, эффективное противодействие ИИ-преступности невозможно без синхронной адаптации национальных законодательств и укрепления международного сотрудничества.

Список литературы

1. Тирранеи В. А. Преступления с использованием искусственного интеллекта // Развитие территорий. 2019. № 3. С. 10–13.
2. Понкин А. В., Редькина А. И. Искусственный интеллект с точки зрения права // Вестник РУДН. Серия: Юридические науки. 2018.
3. Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности. М., 2018.

4. Сафонов А. А. Уголовная ответственность за преступления в сфере высоких технологий. СПб., 2022.
5. Беляев В. Г. Киберпреступность в эпоху искусственного интеллекта. М., 2023.
6. Future of Artificial Intelligence Act of 2017, 115th Congress.
7. Europol Report on AI-enabled Crime. 2023.
8. Materials of case United States v. Vasquez (S.D. Cal. 2024).
9. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. 2024. № 5. С. 149–155.
10. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 г. М. : Московский университет МВД России имени В.Я. Кикотя, 2024. С. 35–37.
11. Константинов А. В. Перспективы развития и использования искусственного интеллекта в целях противодействия преступлениям в сфере информационно-телекоммуникационных технологий / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : сборник научных трудов / сост. А. В. Константинов. М. : Московский университет МВД России имени В.Я. Кикотя, 2023. С. 80–82.
12. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. М. : Ай Пи Ар Медиа, 2025.
13. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий : учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова. М. : Изд-во Юридического института РУТ (МИИТ), 2025.

Савотченко С. Е.¹,

*профессор кафедры высшей математики и физики
Российского государственного геологоразведочного
университета имени Серго Орджоникидзе,
доктор физико-математических наук, доцент*

Симонцев Д. А.²,

*аспирант кафедры высшей математики и физики
Российского государственного геологоразведочного
университета имени Серго Орджоникидзе*

Акапьев В. Л.³,

*доцент кафедры информационно-компьютерных
технологий в деятельности ОВД
Белгородского юридического института
МВД России имени И.Д. Путилина,
кандидат педагогических наук*

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Бурное развитие искусственного интеллекта (далее – ИИ) оказывает значительное влияние на различные аспекты общественной жизни, включая экономику, здравоохранение, образование и безопасность. Например, в экономике использование ИИ позволяет автоматизировать процессы производства и управления, что увеличивает производительность труда и снижает издержки. В здравоохранении ИИ активно применяется для диагностики заболеваний, анализа медицинских данных и разработки новых лекарственных препаратов, что способствует улучшению качества лечения и продлению жизни людей. В образовательной сфере технологии ИИ используются для создания персонализированных программ обучения и анализа прогресса студентов, а в области безопасности – для мониторинга общественного порядка и предотвращения преступлений.

Однако интенсивное внедрение ИИ вызывает множество юридических, этических [1] и социальных вопросов [2]. Например, алгоритмы, применяемые в системах распознавания лиц, могут нарушать право на приватность, а автоматизированные решения в сфере кредитования или найма персонала способны приводить к дискриминации отдельных групп населения. Эти проблемы обостряют необходимость разработки комплексного правового механизма, который обеспечит баланс между развитием инноваций и защитой прав граждан [3]. В условиях

¹ © Савотченко С. Е., 2025.

² © Симонцев Д. А., 2025.

³ © Акапьев В. Л., 2025.

глобальной цифровизации перед Российской Федерацией стоит задача формирования нормативной базы, которая будет способствовать безопасному и ответственному использованию технологий ИИ [5].

Существующее правовое регулирование ИИ в России находится на этапе становления. Оно очень сильно отстает от технологических реалий и возможностей использования ИИ. Несмотря на наличие стратегических документов, таких как Национальная стратегия развития искусственного интеллекта на период до 2030 г., и разработку ряда законодательных инициатив, в правовой системе сохраняются пробелы и недостатки. Изначальная проблема заключается в строгом и однозначном определении понятия ИИ. Этому вопросу посвящено множество появившихся в недавнее время научных публикаций [6–8], включая проблемы выявления признаков ИИ в контексте их использования в правовом поле [9–10].

Одной из ключевых проблем является отставание развития законодательства от стремительного прогресса современных технологий. В то время как ИИ внедряется в новые области и становится все более автономным, правовые механизмы не успевают адаптироваться к возникающим вызовам. Это приводит к тому, что многие аспекты, включая вопросы ответственности за действия ИИ, защиты данных и соблюдения этических норм, остаются неурегулированными. В результате возрастает риск правовой неопределенности, что может тормозить развитие инноваций и снижать уровень доверия общества к технологиям. Возникает необходимость выбора оптимальной модели правового регулирования в сфере искусственного интеллекта [11].

Аналогичная проблема наблюдается в области регулирования криптовалют. Например, законодательство о цифровых активах в России развивается медленно, что создает правовую неопределенность для участников рынка. Введение Федерального закона «О цифровых финансовых активах» (ФЗ-259) в 2020 г. стало значимым шагом, однако многие вопросы, такие как налогообложение, использование криптовалют в качестве платежного средства и меры по предотвращению мошенничества, остаются нерешенными. Это наглядно демонстрирует, что скорость адаптации законодательства к новым технологическим реалиям недостаточна, что создает барьеры для их эффективного внедрения и использования.

Для преодоления данного разрыва требуется системный подход, включающий разработку комплексной нормативной базы, адаптацию международного опыта и внедрение инновационных правовых механизмов. Анализ существующего состояния правового регулирования и поиск эффективных решений являются важными шагами на пути к созданию устойчивой системы регулирования ИИ в Российской Федерации.

Проанализируем основные проблемы правового регулирования ИИ в России.

1. Законодательная база. На сегодняшний день основным нормативным документом, регулирующим развитие ИИ в России, является Национальная стратегия развития искусственного интеллекта (Указ Президента Российской Федерации от 10 октября 2019 г. № 490). Однако эта стратегия носит общий характер и не охватывает все аспекты правового регулирования. В 2020 г. были внесены

изменения в ряд законов, включая Федеральный закон «О персональных данных» (ФЗ-152) и Гражданский кодекс РФ, однако они лишь частично регулируют использование технологий ИИ.

2. Отсутствие единого подхода. В российском законодательстве отсутствует четкое определение ИИ, что затрудняет правоприменение. Это также создает проблемы при разработке специальных нормативных актов, таких как регулирование автономных транспортных средств или использование ИИ в медицинской диагностике. Например, в рамках проекта «Регуляторная гильотина» Минэкономразвития России ведется работа по устранению устаревших норм, но вопрос унификации определений остается нерешенным.

3. Этические и социальные аспекты. Этика и ответственность являются ключевыми вызовами в области регулирования ИИ. Законодательство недостаточно защищает граждан от возможных негативных последствий использования ИИ, включая дискриминацию и нарушения прав на конфиденциальность. В этой связи заслуживает внимания разработка Кодекса этики в сфере ИИ, утвержденного в 2021 г. Ассоциацией больших данных (АБД), однако его нормы пока носят рекомендательный характер.

4. Проблемы адаптации законодательства к новым технологиям. Анализ существующего состояния показывает, что скорость адаптации законодательства к новым технологическим вызовам остается низкой. Это видно на примере других областей, таких как регулирование криптовалют. Медленный процесс принятия необходимых законов и отсутствие четких регламентов затрудняют развитие отрасли и приводят к правовой неопределенности. Подобная ситуация наблюдается и в сфере ИИ, где законодательные инициативы зачастую отстают от реальных потребностей рынка и общества.

5. Международный опыт. Для формирования эффективного регулирования важно учитывать международный опыт. Например, Европейский Союз активно разрабатывает нормативные акты, такие как «Акт об искусственном интеллекте» (Artificial Intelligence Act), который устанавливает четкие правила использования ИИ. Внедрение таких практик в российское законодательство могло бы ускорить процесс адаптации и повысить конкурентоспособность страны.

Выделим следующие основные направления и перспективы совершенствования правового регулирования.

1. Разработка унифицированного определения ИИ. Введение юридически значимого определения ИИ является первым шагом к созданию целостной нормативной базы. Такое определение должно учитывать многообразие технологий и сфер применения ИИ. В качестве примера можно привести инициативы Евразийской экономической комиссии, направленные на согласование подходов к регулированию ИИ на пространстве ЕАЭС.

2. Установление ответственности. Необходимо разработать механизмы определения ответственности за действия ИИ, включая случаи, когда системы принимают автономные решения. Это может включать внедрение концепции «ответственности оператора» или производителя технологии. Например, в рамках Федерального закона «О экспериментальных правовых режимах в сфере цифровых инноваций» (ФЗ-258) уже создаются условия для тестирования таких подходов.

3. Обеспечение защиты персональных данных. Системы ИИ работают с большими объемами данных, что повышает риски утечки и неправомерного использования информации. Усиление регулирования в этой сфере должно предусматривать строгие требования к сбору, хранению и обработке данных. Важно учитывать положения Общего регламента по защите данных (GDPR) Европейского Союза, адаптируя их к российским реалиям.

4. Регулирование этических аспектов. Следует разработать этические стандарты использования ИИ, которые будут включать принципы недискриминации, прозрачности и объяснимости решений ИИ. Создание специализированных этических комитетов при государственных органах может способствовать реализации этих стандартов. В качестве ориентира можно использовать рекомендации ЮНЕСКО, принятые в 2021 г.

5. Гармонизация с международными нормами. Важно учитывать международный опыт, включая разработки Европейского Союза в области регулирования ИИ, такие как проект «Акт об искусственном интеллекте» (Artificial Intelligence Act). Применение лучших практик позволит повысить конкурентоспособность России на мировом рынке технологий.

6. Разработка специализированных правовых режимов. Введение экспериментальных правовых режимов («регуляторных песочниц») в сфере ИИ позволит протестировать новые технологии и нормативные подходы в ограниченных условиях. Такие меры позволят выявить потенциальные риски и недостатки до их масштабного внедрения.

7. Усиление межведомственного взаимодействия. Для успешной реализации нормативных инициатив требуется координация между различными органами государственной власти, научными учреждениями и бизнес-сообществом.

Таким образом, совершенствование правового регулирования ИИ в Российской Федерации требует комплексного подхода, который будет учитывать как внутренние, так и международные реалии. Основными направлениями реформ должны стать разработка четкой законодательной базы, регулирование ответственности и этических аспектов, а также защита прав граждан. Успешная реализация этих мер обеспечит развитие технологий ИИ в интересах общества и государства, минимизируя возможные риски [12].

Для успешной реализации комплексного подхода целей необходимо:

- разработать единое определение ИИ в законодательстве;
- установить принципы ответственности за действия ИИ и автономных систем;
- усилить защиту персональных данных и права граждан на приватность;
- внедрить обязательные этические стандарты использования ИИ;
- активизировать участие России в международных инициативах по регулированию ИИ;
- развивать механизмы экспериментальных правовых режимов.

Только такой системный и сбалансированный подход позволит создать эффективную правовую основу, которая будет способствовать инновационному развитию и защите интересов общества.

Список литературы

1. Петрова Е. В. Этические проблемы искусственного интеллекта в правовом контексте // Вестник права. 2022. № 4. С. 45–52.
2. Кузнецова Л. П. Искусственный интеллект и права человека: анализ существующих проблем // Государство и право. 2023. № 8. С. 17–25.
3. Сидоров А. В. Регулирование искусственного интеллекта в Российской Федерации: вызовы и перспективы // Журнал российского права. 2023. № 6. С. 23–30.
4. Филипова И. А. Правовое регулирование искусственного интеллекта. Н. Новгород : Нижегородский госуниверситет, 2025.
5. Кобец П. Н. Искусственный интеллект: современные подходы по формированию понятийного аппарата и регулированию правоотношений в рассматриваемой сфере // Вестник Самарского юридического института. 2023. № 5 (56). С. 30–37.
6. Минбалеев А. В. Понятие «искусственный интеллект» в праве // Вестник Удмуртского университета. Серия Экономика и право. 2022. Т. 32. № 6. С. 1094–1099.
7. Чеботарева А. А., Керопян Ю. П. Подходы к определению понятия искусственного интеллекта: постановка проблемы // Юридический мир. 2023. № 2. С. 38–42.
8. Филипова И. А. Искусственный интеллект, робот и нейротехнологии: понятие, соотношение и пределы правового регулирования // Государство и право. 2024. № 4. С. 148–158.
9. Мансуров Г. З. Понятие и признаки искусственного интеллекта // Право и государство: теория и практика. 2023. № 11 (227). С. 286–287.
10. Соломонов Е. В. Понятие и признаки искусственного интеллекта // Вестник Омского университета. Серия «Право». 2023. Т. 20. № 4. С. 57–65.
11. Арзамасов Ю. Г. Оптимальная модель правового регулирования в сфере искусственного интеллекта // Вестник Воронежского государственного университета. Серия: Право. 2023. № 2. С. 133–148.
12. Медведев А. И. Принцип прозрачности искусственного интеллекта в системе принципов российского права // Вестник Удмуртского университета. Серия Экономика и право. 2023. Т. 33. № 3. С. 516–526.

Савченко Е. А.¹,
*научный сотрудник отдела
социального законодательства Института
законодательства и сравнительного
правоведения при Правительстве Российской Федерации,
кандидат юридических наук*

ПРАВОВЫЕ АСПЕКТЫ СОЦИАЛЬНОГО НЕРАВЕНСТВА, СВЯЗАННЫЕ С «РАЗНОУРОВНЕВЫМ» ДОСТУПОМ К ВОЗМОЖНОСТЯМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Президент Российской Федерации В. В. Путин в ходе выступления на пленарной сессии Петербургского международного экономического форума (ПМЭФ) в 2023 г. подчеркнул, что «социальная справедливость является одним из принципов развития экономики Российской Федерации», неукоснительное соблюдение которого должно вести к сокращению неравенства. Рост научно-технологического потенциала экономики должен вести к сокращению неравенства, а не к его усугублению. При этом глава государства добавил, что Россия «не является чемпионом по решению этих задач», остается много вопросов.

Как подчеркнул позже, в 2024 г. на Петербургском международном юридическом форуме (ПМЮФ), Председатель Конституционного суда Российской Федерации В. Д. Зорькин одним из важнейших вопросов развития искусственного интеллекта (далее – ИИ), является «проблема возрастающего социального неравенства и расслоения, связанная с “разноуровневым” доступом к возможностям ИИ» [1].

Академик Т. А. Хабриева акцентирует, что «во всем мире наблюдается нарастание правового регулирования» ИИ [2], в то же время нельзя не согласиться с точкой зрения профессора Ю. А. Тихомирова, что «законодательное регулирование “не успевает” за развитием отношений» в сфере искусственного интеллекта, служит средством их “запоздалого” регулирования, не оказывает опережающего воздействия» [3].

В выступлениях ученых на международной междисциплинарной конференции «Философия искусственного интеллекта – искусственный интеллект и сознание», которая была организована Российской академией наук, Научным советом при Президиуме РАН по методологии ИИ и когнитивных исследований вместе с Центром искусственного интеллекта МГИМО и рядом российских и зарубежных образовательных и исследовательских организаций подчеркивалось, что вопросы регулирования использования искусственного интеллекта – проблематика широкого, межотраслевого характера не только правовых наук.

На конференции были рассмотрены вопросы феномена ИИ, например, как возможности перспективного технологического усовершенствования, а также были подняты вопросы необходимости определения границ применимости ИИ,

¹ © Савченко Е. А., 2025.

проблем безопасности, защиты персональных данных и международного правового регулирования.

Рассматривая юридическую проблематику использования искусственного интеллекта, ученые отмечают: необходимость «при использовании ИИ в государственном управлении нормативно закрепить принцип прозрачности (транспарентности)» [4], урегулирования таких вопросов, как манипуляция в процессе обработки информации персонифицированного характера (персональных данных), возможности контроля за поведением индивида, прежде всего в сети Интернет [5], развитие эмоционального искусственного интеллекта, введение так называемого социального рейтинга и др. [6], необходимость «создавать законодательство, которое будет обеспечивать надлежащую защиту прав и свобод человека» при использовании искусственного интеллекта [7].

Как отмечает профессор Н. С. Бондарь «формирующееся информационно-цифровое пространство – качественно новая сфера правового, в том числе конституционно-правового, влияния» [8].

Главная опасность использования искусственного интеллекта состоит все же не только в том, что люди станут думать, как компьютеры, но и в том, что в силу независимых от граждан причин не все будут иметь возможность реализовать в своей повседневной жизни свое право на использование ИИ.

Перед продолжением дальнейшего анализа необходимо отметить, что в соответствии с изменениями, внесенными Указом Президента Российской Федерации от 15.02.2024 № 124 в Национальную стратегию развития ИИ (далее – Стратегия), «искусственный интеллект» – это не только комплекс технологических решений, который позволяет имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, не только сопоставимые с результатами интеллектуальной деятельности человека, но и превосходящие их.

В своем докладе в рамках Всероссийской междисциплинарной конференции «Философия искусственного интеллекта» на секции «Искусственный интеллект и право» директор Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, академик РАН Т. Я. Хабриева подчеркнула, что сейчас под эгидой ООН запущен процесс конструирования международно-правовой матрицы искусственного интеллекта.

Важное значение для построения регулирования искусственного интеллекта имеют Глобальный цифровой договор, принятый Генеральной ассамблеей ООН в 2022 г., а также Доклад ООН о регулировании ИИ, опубликованный 19.09.2024, и в котором предлагается создать независимую Международную научную группу по ИИ.

Необходимо отметить, что развитие ИИ в настоящее время невозможно без использования ресурсов Интернет, где десятки миллионов пользователей, используя разные инструменты ИИ, фактически обеспечивают его обучение и развитие. Глобальный цифровой договор – это документ «мягкого права», в котором отмечается:

– необходимость международного сотрудничества в целях устранения цифровых разрывов между странами и внутри них;

- необходимость выявлять и уменьшать риски и обеспечивать надзор за технологиями со стороны человека таким образом, чтобы это способствовало устойчивому развитию и полному осуществлению прав человека;

- необходимость цифрового сотрудничества, которое основано на нормах международного права, включая Устав ООН, международное право в области прав.

В части четвертой ГК РФ под базой данных понимается представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

Однако понятие информационно-коммуникационная инфраструктура в законодательстве отсутствует. В Стратегии всего лишь отмечается, что «дополнительными благоприятными факторами развития технологий искусственного интеллекта в России являются современная базовая информационно-коммуникационная инфраструктура». Это имеющийся в России высокий уровень доступа к сети Интернет, доступность мобильной передачи данных и развитые сети радиотелефонной связи 3-го и 4-го поколений.

Однако, несмотря на широкое использование понятия «Интернет» в российском законодательстве единого легального определения этого понятия до сих пор нет.

В Концепции развития информационно-коммуникационной инфраструктуры и технологий в Российской Федерации информационно-коммуникационная инфраструктура указывается, как совокупность информационных (определяемых, как взаимосвязанная совокупность информационных систем и подсистем) и коммуникационных инфраструктур.

Коммуникационная инфраструктура, в свою очередь, определена, как сетевая инфраструктура, обеспечивающая передачу информации между территориально распределенными источниками и получателями, состоящая из линий связи, использующих различные среды распространения электромагнитных сигналов и оборудования, обеспечивающего прием, передачу этих сигналов, и их обработку в процессе этой передачи.

Возвращаясь к теме нашей статьи и проанализировав состав понятия «искусственный интеллект», под разноуровневым доступом к возможностям ИИ, по мнению автора, необходимо считать:

- уровень доступа к возможностям ИИ, обеспечиваемый в первую очередь уровнем доступа к сети Интернет, и, соответственно, развитием коммуникационной инфраструктуры;

- разноуровневость во владении навыками использования ИИ (навыки);

- дифференциацию во владении навыками использования ИИ свидетельствует о неравных возможностях индивидов (использование).

В соответствии с п. 4 ст. 2 Закона об информации под информационно-телекоммуникационной сетью понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

В ст. 2 Модельного закона (об основах регулирования Интернета) Интернет определяется как глобальная информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанная на использовании комплексов интернет-протоколов и протокола передачи данных и предоставляющая возможность реализации различных форм коммуникации.

Ученые, исследующие возможности и правовое регулирование современных информационных технологий, подчеркивают, что только при наличии всеобщего минимального права на доступ в Интернет гарантирована реализации права на информацию и что «мы накануне международного признания нового фундаментального права – права на доступ в Интернет» [8]. По мнению данных ученых, это право должно, основываясь на возможностях современной информационно-коммуникационной инфраструктуры с обязательной сетевой и технологической нейтральностью, запретом дискриминации сетевого трафика, обеспечивать максимальный охват для доступа к сети Интернет.

По ГОСТ Р 55387-2012 под услугой «доступ в Интернет» понимается совокупность действий оператора связи по подключению оконечного оборудования или локальной сети пользователя к сети оператора и обеспечению возможности доступа пользователю к ресурсам и услугам Интернет (веб-службам, передаче файлов по протоколу FTP и др.). Подробное нормативное регулирование доступа к сети Интернет содержится в Правилах телематических услуг связи и в Правилах услуг по передаче данных. Доказывание отсутствия технической возможности для предоставления доступа к сети передачи данных лежит на операторе связи (абз. 4 п. 22, п. п. 23, 24 Правил телематических услуг связи).

Необходимо отметить, что в настоящее время легального общепринятого определения телематических услуг связи в российском законодательстве также нет. Например, в Определении Верховного Суда РФ от 12.12.2013 № АПЛ13-538 указано, что телематические услуги связи – это любые услуги связи, предусматривающие использование кибернетического пространства. Одним из видов оказания этих услуг является, в частности, предоставление доступа к сети Интернет. Более ограниченным является определение, сформулированное в ФАС России службе, например, в решениях Магаданского УФАС России от 21.12.2016 по делу № 04-30/143-2016, Приморского УФАС России от 29.05.2018 № 476/04-2018, в частности, отмечается: телематические услуги связи – это комплекс услуг, которые оператор предоставляет клиентам в части электронных коммуникаций, с присвоением каждому из них кода идентификации (адреса).

По мнению автора, телематические услуги связи – это:

- услуги связи, оказываемые оператором на основании соответствующей лицензии в соответствии с договором, заключенным с абонентом;
- с присвоением абонентам кода идентификации и обеспечивающие;

- доступ к информационным системам информационно-телекоммуникационных сетей, в том числе к сети Интернет;
- прием и передачу телематических электронных сообщений, передачу сигналов оповещения и экстренной информации об опасностях, связанных с чрезвычайными ситуациями.

Что касается услуг связи по передаче данных, то нужно отметить, что такие услуги подразделяются:

- на услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации;
- и услуги связи по передаче данных для целей передачи голосовой информации.

Легального определения услуги связи по передаче данных в России в настоящий период времени также нет. В соответствии с утратившим силу внутренним документом «Сети и службы передачи данных», утвержденным Приказом Министерства РФ по связи и информатизации от 12.11.2001 № 225 под сетью передачи данных понималась – совокупность узлов и каналов электросвязи, специально созданная для организации связей между определенными точками с целью обеспечения передачи данных между ними.

На основе анализа законодательства о связи можно сказать, что передача данных – это перенос данных в виде сигналов от точки источника информации к ограниченному или неограниченному числу получателей, находящихся на расстоянии, современными средствами связи по каналам передачи данных, для последующей обработки средствами вычислительной техники.

В постановлении Правительства Российской Федерации от 24.11.2014 № 1240 дается определение сети передачи данных органов власти, которые определяются как элемент инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, в целях осуществления государственных функций.

В этой связи необходимо отметить, что по Федеральному закону «О связи» (далее – Закон о связи) на операторов связи, оказывающего услуги по предоставлению доступа в Интернет, возложена обязанность обеспечивать без взимания платы доступ к отечественным социально значимым информационным ресурсам, в число которых включены единый портал государственных и муниципальных услуг (Госуслуги) и социальная сеть «ВКонтакте».

Как отмечается в отчете Ericsson о мобильности, объем передачи данных в сетях мобильной связи в странах Западной Европы в 2017–2024 гг. вырос в расчете на 1 смартфон с 3,05 до 22,46 гб/месяц, в странах Центральной и Восточной Европы с 2,73 до 19,48 гб/месяц. Еще более высокий рост – до 31,88 гб/месяц в Индии, Непале и Бутане. При этом операторы мобильной связи в нашей стране работают в условиях дефицита доступного радиочастотного ресурса по сравнению с крупнейшими иностранными рынками мобильной связи. В международном рейтинге GSMA – организации, объединяющей операторов мобильной связи – Mobile Connectivity Index (Индекс мобильного взаимодействия) Российская Федерация в 2023 г. заняла 45 позицию из 173. Отметим, что в 2014 г. Россия была на 36

(в 2017 – на 34). В значительной мере снижение позиции нашей страны произошло из-за задержки появления широкодоступной сотовой сети пятого поколения, обусловленной санкционным давлением стран Запада, поэтому разноуровневый доступ к возможностям искусственного интеллекта будет сохраняться.

Основными рисками разноуровневого доступа к возможностям искусственного интеллекта являются ограничения осуществления определенной жизненной стратегии индивида, полноценного участия в жизни общества, личностного роста и расширения социальных связей и отношений, а также демократического участия.

Рассматривая вопрос о социальном неравенстве, связанном с «разноуровневым» доступом к возможностям искусственного интеллекта, нельзя оставить без внимания Концепцию цифровой и функциональной трансформации социальной сферы до 2025 г., которая «изначально постулирует установки экономического и технологического детерминизма применительно к социальной сфере» [9].

В Концепции трансформации социальной сферы предусматривается внедрение искусственного интеллекта, в том числе для заключения социального контракта с малоимущими семьями.

Однако, как справедливо отмечают авторы, «ориентация на внедрение искусственного интеллекта во все сферы правового сопровождения социальной жизни рискует обернуться стагнацией в развитии права, лишая человека стимулов к аналитическому мышлению» [10].

Подводя итог, сделаем следующие выводы, чтобы решить вопрос социального неравенства, связанного с «разноуровневым» доступом к возможностям искусственного интеллекта:

1. Необходимо, прежде всего, решить проблему «терминологического вакуума», а именно дать легальное определение понятий информационно-коммуникационная инфраструктура, Интернет, телематических услуг связи и услуги связи по передаче данных в российском законодательстве.

2. В первую очередь для граждан, которые имеют право на льготы и меры социальной поддержки, очень важно создать программы обучения на федеральном уровне.

3. Перечень отечественных социально значимых информационных ресурсов необходимо расширить, например, включить уже созданные информационные ресурсы в сфере культуры.

4. Внести изменения в Стратегию, пункт «з» дополнить после слов «информирование граждан и организаций о принципах использования технологий искусственного интеллекта» и организация обучения использованию технологий искусственного интеллекта для граждан, которые имеют право на льготы и меры социальной поддержки.

Анализируя вышесказанное, можно сделать вывод, что разноуровневый доступ к возможностям искусственного интеллекта будет сохраняться как минимум до появления широкодоступной сотовой сети пятого поколения. Однако у любого минуса есть и свои плюсы, например, вынужденный постепенный переход к возможностям искусственного интеллекта позволит сохранить стимулы к аналитическому мышлению.

Список литературы

1. Зорькин В. Право и вызовы искусственного интеллекта // Офиц. сайт газеты «Российская газета». – 2024. – 27 июня. – Электронная публикация. URL: <https://rg.ru/2024/06/27/pravo-i-vyzovy-iskusstvennogo-intellekta.html>.
2. Интервью с академиком Т. Я. Хабриевой «Искусственный интеллект сквозь призму права». URL: <https://scientificrussia.ru/articles/iskusstvennyj-intellekt-skvoz-prizmu-prava-intervu-s-akademikom-taliej-habrievoj>.
3. Тихомиров Ю. А. Методология анализа и оценки рисков в законодательной деятельности // Юридическая техника. 2015. № 9.
4. Талапина Э. В. Принцип прозрачности использования искусственного интеллекта // Государственная власть и местное самоуправление. 2024. № 7. С. 36–39.
5. Авакьян С. А. Информационное пространство знаний, цифровой мир и конституционное право / // Конституционное и муниципальное право. 2019. № 7. С. 23–28.
6. Ковалева Н. Н. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта / Н. Н. Ковалева, Н. А. Жирнова // Журнал российского права. 2024. № 7. С. 109–121.
7. Виноградов В. А. Правовые аспекты развития систем искусственного интеллекта // Закон. 2023. № 12. С. 157–166.
8. Бондарь Н. С. Информационно-цифровое пространство в конституционном измерении: из практики Конституционного Суда Российской Федерации // Журнал российского права. 2019. № 11. С. 25–42.
9. Талапина Э. В. Право на информацию в свете теории субъективного публичного права // Сравнительное конституционное обозрение. 2016. № 6 (115). С. 81 ; Щербович А. А. Реализация конституционных прав и свобод в Интернете. М. : ТЕИС, 2015.
10. Обеспечение прав человека и осуществление публичной власти в современных условиях: проблемы и решения: монография / под ред. Т. А. Васильевой, Н. В. Варламовой. М.: ИГП РАН, 2023.

Смушкин А. Б.¹,
 доцент кафедры криминалистики
 Саратовской государственной
 юридической академии,
 кандидат юридических наук, доцент

ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦИФРОВЫХ ПЛАТФОРМ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

В условиях активной цифровой трансформации раскрытия, расследования и предупреждения преступлений необходимо уделить внимание также исследованию ближайших перспектив развития цифровых платформ.

Следует отметить, что использование изолированных платформ правоохранительных органов снижает уровень эффективности данной технологии. В ходе анкетирования, отсутствие единой цифровой платформы отметили 15,2 % опрошенных ученых как одну из основных проблем, мешающих цифровой трансформации расследования. При этом 85,9 % опрошенных ученых согласны с необходимостью развития отдельных цифровых платформ и информационных порталов правоохранительных органов в единую экосистему.

Развитие цифровых платформ может идти двумя основными путями:

1. Соединение существующих платформ программными шлюзами (Интеграция платформ с помощью горизонтальных связей).
2. Кроссплатформенное объединение современных цифровых платформ путем их слияния в единой программной оболочке.
3. Взаимная интеграция цифровых платформ в единую экосистему правоохранительных органов. с включением в нее только баз данных существующих платформ. Экосистема правоохранительных органов может включить в себя как открытые, так и закрытые платформы.
4. Создание полностью новой экосистемы.

Каждый из путей имеет своих сторонников, а также аргументы *pro et contra*. Проведенный опрос научно-педагогических сотрудников- представителей наук криминального цикла, показал, что сторонники разных форм объединения представлены в следующем соотношении:

- кроссплатформенное объединение цифровых платформ правоохранительных органов в единый комплекс – 31,7 %;
- разработка полностью новой экосистемы – 28.6 %;
- разработка надстройки над функционирующими платформами, позволяющей использование их через единый портал – 19 %;
- организация горизонтальных связей (шлюзов) без объединения платформ – 9.5 %;
- 11.1 % затруднились ответить.

Так, в качестве аргумента о невозможности объединения цифровых платформ в единую экосистему, А. Ю. Чурикова отмечает, что «у цифровой платформы,

¹ © Смушкин А. Б., 2025.

если ее рассматривать не как платформенное решение, позволяющее создавать децентрализованные интегрируемые информационные системы, а как некий отдельный самостоятельный ресурс, должен быть единый оператор. Возможно ли в сфере уголовного судопроизводства выделить орган, который бы стал единым оператором цифровой платформы и это не нарушило бы принципы уголовного процесса и не перегрузило бы данный орган несвойственной ему работой? Считаем, что нет. На эту роль с учетом обозначенных критериев не подходят ни ВС РФ, ни Генеральная прокуратура, ни СК, ни МВД» [1, с. 110]. Она полагает, что «целесообразным представляется не создание отдельной общей мега-системы, а обеспечение техническими и правовыми мерами интегрируемости и взаимодействия между эксплуатируемыми разными участниками уголовного процесса информационными системами» [1, с. 112].

Кроссплатформенное объединение в единой программной оболочке представляется слишком громоздким конструктом, для которого вряд ли будут достаточными технические характеристики оборудования в регионах, особенно вне расположения областных центров. К тому же, оборудование и телекоммуникационные каналы будут явно перегружены не нужной для данного информацией, потребляющей и так не слишком большие ресурсы. При этом нельзя не отметить техническую сложность подобной интеграции. Цифровые платформы каждого ведомства имеют свои стандарты и структуру. Кроме того, явно возникнет проблема совместимости данных, поскольку в разных ведомствах используются разные платформы на базе разного аппаратно-программного обеспечения. Для объединения разных платформ, разработанных в разное время под разные задачи, может потребоваться реинжиниринг, что по финансовым и временным затратам окажется не экономичнее следующих двух вариантов. При объединении платформ может возникнуть необходимость упрощения или отказа от некоторых функций, чтобы обеспечить совместимость и унификацию. Кроме того, желательно чтобы для пользователя сложное, интегрированное сквозное взаимодействие платформ выглядело бесшовным. Подобное кроссплатформенное централизованное объединение может стать более уязвимым к кибератакам.

Разработка абсолютно новой экосистемы, безусловно, помогла бы решить многие накопившиеся проблемы, избежать ряда ошибок, выявленных в современных платформах, учесть все, высказываемые теоретиками и практиками замечания и предложения, буквально сработать на перспективу, однако период начала ввода в эксплуатацию и адаптации к ней правоохранительных органов может отличаться повышенным количеством проблем. Финансовые затраты на разработку и внедрение этой новой экосистемы необходимо будет нести практически с нуля. Кроме того, пытаясь избежать старых ошибок, разработчики не гарантированы от совершения новых, методы исправления которых нужно будет разрабатывать от самых основ. Во время внедрения этой системы явно будет период, когда старые платформы не работают уже, а новая экосистема еще. Также сложно спрогнозировать нагрузку пользователей на эту экосистему, поскольку, в нашей трактовке, кроме властных субъектов уголовного процесса (число которых еще можно учесть), доступ к некоторым элементам функционала экосистемы должны иметь и иные заинтересованные лица.

На настоящий момент мы полагаем объединение ресурсов более оптимальным путем повышения эффективности цифровых платформ правоохранительных органов, чем автономное использование, пускай и пронизанное горизонтальными связями, создание кроссплатформенного объединения. При этом объединение ресурсов должно быть не прямым синтезом цифровых платформ каждого ведомства в единый программный комплекс, а разработкой программной общей среды обмена информацией- мастер-платформы. Складывающаяся общая среда обмена информацией будет выступать как надстройка, как некий объединяющий фактор. При этом фактически решается вопрос о едином операторе этой экосистемы. Поскольку операторы цифровых платформ каждого ведомства при этом меняться не будут, единый общий оператор будет обеспечивать именно функционирование этой общей среды, надстройки. Следовательно, оператором может стать государственная некоммерческая организация, в функции которой может входить обеспечение функционирования сервера, являющегося центральным хабом сети распределенной информации и обеспечивающего обмен информацией напрямую между ведомствами. Однако, безусловно, скорость работы подобной системы будет зависеть от работы отдельных платформ, что может заметно замедлять доступ к данным.

Поэтому параллельно с функционированием этой межплатформенной экосистемы возможна постепенная разработка полностью новой экосистемы уголовного судопроизводства, обеспечивающей движение электронного уголовного дела от подачи заявления, до вступления в силу судебных решений. Разрабатывать необходимо новую экосистему с проверкой ее в «песочнице» в одном двух регионах, наймом «белых хакеров» для поиска ошибок и проверки кибербезопасности (пентестинга). Конечно, в предлагаемом варианте решения вопроса получается двойная работа и повышенные материальные затраты. Однако, как нам представляется, изменения в сфере уголовного судопроизводства не просто назрели, а буквально «перезрели», при том, что кардинальная ломка существующих структур и внедрение «не отшлифованных» технологий и концептов может привести к непоправимым последствиям. Единым же оператором, по мнению большинства опрошенных (49,2 %) должна стать новая, образованная для этих целей структура. Решение проблемы определения единого оператора цифровой экосистемы должно лежать в контексте создания государственной некоммерческой организации, в функции которой будут входить обеспечение автоматизированной обработки информации и обеспечение доступа к этой информации. Кроме того, следует учитывать возможность использования технологии частично распределенной информации (аналогичной принципам работы BitTorrent), при которой единый HTTP сервер, управляемый единым общим оператором, организует связь модулей, управляемых ведомственными операторами между собой. Подобный подход с использованием распределенных реестров снизит нагрузку на оборудование единого оператора (и, соответственно – требования к нему). При этом, общий оператор будет фактически только направлять векторы движения информационных потоков, что обуславливает отсутствие необходимости получения допуска к конфиденциальной информации со стороны его сотрудников.

При построении рассматриваемой экосистемы нам представляется обоснованным рекомендовать использование именно отечественных программных оболочек и технологий. Это не только решает вопрос импортозамещения, но и обезопасит систему от «вписывания» в нее несанкционированных способов доступа (Backdoor) авторов или иных заинтересованных лиц (или спецслужб).

Архитектура экосистемы должна реализовывать принцип модульности. Модульную структуру достаточно обоснованно и полно описал В. В. Тюрин как «концепцию архитектуры информационной системы, предусматривающей в качестве основной модели ее исполнения совокупность интегрированных между собой условно-независимых программных модулей, каждый из которых выполняет определенную функцию, имеет свою защищенную логику реализации и программный интерфейс для взаимодействия» [2, с. 112]. При этом представляется разумным использование программ-клиентов цифровой экосистемы, устанавливаемых на аппаратуре правоохранительного органа. С помощью клиента можно регулировать объем модулей, к которому получает доступ данный орган, что существенно может разгрузить информационные мощности от непрофильной информации и увеличить быстродействие системы. С учетом предлагаемой нами модульной структуры экосистемы представляется эффективным использование технологии контейнеризации, при которой каждое приложение со всеми зависимостями упаковывается в отдельный стандартный программный блок, использование которого возможно в любой среде. Кроме того, при разработке новой экосистемы правоохранительных органов эффективно будет использовать микросервисную архитектуру в который каждый из небольших сервисов выполняет элемент функции или небольшую функцию.

Ранее мы уже обозначали схему построения предлагаемой экосистемы: «единая стержневая основа, содержащая необходимые для каждого органа и его отдела элементы; подключаемые через установленный интерфейс ведомственные блоки (технически блоки могут быть реализованы по-разному); функциональные модули, необходимые для работы конкретных целевых отделов (по борьбе с экономическими преступлениями, с незаконным оборотом наркотиков и т. д.), а также применяемые конкретными сотрудниками при использовании в структуре организационного принципа специализации» [3, с. 1028].

Таким образом, представляется неминуемой эволюция цифровых платформ в единую экосистему уголовного судопроизводства, организованную по модульному принципу. Оператором данной платформы может стать государственная некоммерческая организация.

Список литературы

1. Чурикова А. Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование : дис. ... д-ра юрид. наук. Саратов, 2024.
2. Тюрин В. В. Управление цифровой трансформацией. Основные тезисы и понятия / Владислав Владимирович Тюрин. – [б. м.] : Издательские решения, 2023.

3. Савельева М. В., Смушкин А. Б., Солдаткина О. Л. Системный подход к единой экосистеме уголовного судопроизводства на основе цифровой платформы // Вестник Санкт-Петербургского университета. Право. 2024. № 4. С. 1026–1042.

Соломатина А. Г.¹,
*доцент кафедры противодействия
преступления в сфере
информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ИНСТРУМЕНТЫ И ТЕХНОЛОГИИ ДЛЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С КРИПТОВАЛЮТАМИ: АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ И ПЕРСПЕКТИВ РАЗВИТИЯ

Криптовалюты, обладая свойствами децентрализации, псевдоанонимности и трансграничности, сформировали принципиально новую среду для противоправной деятельности, поставив перед правоохранительными органами задачи, требующие адаптации традиционных методов расследования к цифровой реальности. Согласно данным Росфинмониторинга, в 2024 г. ущерб от краж криптовалют в России превысил 15 млрд рублей, при этом лишь 23 % таких преступлений были раскрыты, что подчеркивает системные сложности в противодействии данным видам правонарушений. Основная проблема заключается в диссонансе между технологической сложностью криптоактивов и ограниченностью правовых механизмов их регулирования, что создает почву для латентности преступлений и затрудняет процесс доказывания.

Современные инструменты расследования криптовалютных преступлений базируются на сочетании блокчейн-анализа, крипто-форензики и межведомственного взаимодействия.

Технологические платформы типа Chainalysis Reactor и Elliptic Investigator, используя графовый анализ, позволяют визуализировать транзакционные цепочки, идентифицируя кластеры кошельков, ассоциированных с незаконной деятельностью. Например, в рамках расследования хищения 2,5 млн рублей через сеть криптоматов в 2024 г. МВД России успешно применило систему Crystal Blockchain для отслеживания перемещения средств от терминалов до бирж Binance и Bybit, что стало возможным благодаря деанонимизации IP-адресов операторов и сопоставлению временных меток транзакций. Параллельно внедрение Росфинмониторингом системы «Прозрачный блокчейн» позволило автоматизировать проверку кошельков по базам санкционных списков, выявив за первый год эксплуатации 120 цифровых адресов, связанных с финансированием терроризма.

Однако технологические решения сталкиваются с непрерывным усложнением методов противодействия со стороны злоумышленников. Широкое использование миксеров (Tornado Cash, Wasabi Wallet), обеспечивающих анонимиза-

¹ © Соломатина А. Г., 2025.

цию 89 % транзакций в Darknet, а также протоколов типа SilentPayment, маскирующих получателя средств, существенно затрудняет отслеживание денежных потоков. В 2024 г. 45 % расследований столкнулись с невозможностью дешифровки данных из-за применения алгоритмов постквантовой криптографии, что актуализирует необходимость разработки инструментов на базе искусственного интеллекта. Нейросетевые модели, такие как Chainalysis KYT, демонстрируют потенциал в прогнозировании перемещения средств с точностью до 93 %, анализируя паттерны поведения и коррелируя их с известными схемами отмывания.

Правоприменительная практика в России сталкивается с комплексом юридических коллизий, усугубляемых отсутствием единообразного подхода к квалификации преступлений. Несмотря на признание криптовалюты имуществом в соответствии с Федеральным законом № 672-ФЗ (2023 г.), сохраняется правовая неопределенность в вопросах конфискации и экстрадиции. Так, в 67 % случаев изъятия холодных кошельков доступ к активам оставался невозможен из-за отсутствия приватных ключей, что ставит под сомнение эффективность мер процессуального принуждения. Дискуссия о применении ст. 159 (мошенничество) или ст. 158 (кража) УК РФ к случаям взлома криптокошельков, как в деле о хищении средств с Trezor (2024 г.), отражает потребность в специализированных нормах, учитывающих специфику цифровых активов.

Бесспорно, при расследовании таких преступлений в первую очередь следует обратить внимание на проблемы международного сотрудничества и оказания правовой помощи. Децентрализованные биржи (Uniswap, PancakeSwap), не требующие KYC-верификации, а также юрисдикционная раздробленность осложняют взаимодействие с иностранными платформами. В деле о фишинговой атаке на поддельный сайт PancakeSwap, где было похищено 890 млн рублей, 70 % средств не удалось восстановить из-за отсутствия механизмов принудительного возврата активов с офшорных бирж, таких как KuCoin. Это подчеркивает необходимость укрепления международных соглашений в духе проекта ОЭСР (2025 г.), предусматривающего автоматический обмен данными между FinCEN и Росфинмониторингом, а также создание единого AML-стандарта для транзакций свыше 1000 USD.

Кадровый дефицит и недостаточная техническая подготовка следователей усугубляют ситуацию. По данным Следственного комитета РФ, лишь 12 % сотрудников обладают компетенциями для работы с блокчейн-эксплорерами, что приводит к зависимости от внешних экспертов и увеличивает сроки расследования на 40 %. Отсутствие профильных подразделений в регионах вынуждает централизовать расследования, создавая узкие места в процессуальных цепочках. В этой связи инициатива МВД России по созданию межведомственных криптолабораторий, оснащенных квантово-безопасными алгоритмами (NTRUEncrypt) и sandbox-средами для симуляции атак, представляется стратегически важной.

Перспективы развития крипто-криминалистики связаны с синтезом технологических инноваций и правовых реформ. Проект поправок в УПК РФ (2025 г.), включающий стандарты изъятия аппаратных кошельков (ст. 164.1) и обязательную регистрацию DEX-платформ (ст. 15.4 ФЗ «О ЦФА»), направлен на устране-

ние пробелов в действующем законодательстве. Одновременно внедрение цифровых двойников для моделирования атак и разработка национального реестра крипто-кошельков позволят минимизировать риски утечек данных.

В заключение следует отметить, что эффективное противодействие крипто-преступности требует не только технологической модернизации, но и гармонизации правовых систем на международном уровне. Реализация предложенных мер, включая унификацию законодательства, подготовку специалистов и внедрение AI-решений, способна сократить уровень крипто-преступности на 35–40 % к 2030 г., обеспечив защиту как публичных, так и частных интересов в цифровом пространстве.

Список литературы

1. Федеральный закон от 25.12.2023 № 672-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 52 (ч. I). Ст. 8951.
2. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31. Ст. 5023.
3. Chainalysis. The 2024 Crypto Crime Report // URL: <https://go.chainalysis.com/2023-crypto-crime-report.html>.
4. Редькин А. В. Проблемы конфискации криптовалют в уголовном процессе // Вестник Московского университета. Серия 11. Право. 2024. № 3. С. 45–59.
5. Осипов Г. И. Анализ ущерба от краж криптовалют в РФ // Финансовая аналитика: проблемы и решения. 2025. № 2. С. 12–18.
6. Интервью с представителем Следственного комитета Российской Федерации // Официальный сайт Следственного комитета РФ. URL: <https://sledcom.ru>.
7. Миненкова А. А. Криптовалюта как объект уголовно-правовой защиты. М. : Юрлитинформ, 2024.
8. Руководство Росфинмониторинга № 12-2024 «О применении системы "Прозрачный блокчейн"» // Официальный сайт Федеральной службы по финансовому мониторингу. URL: <https://fedsfm.ru/documents/guide/12-2024>.
9. Руководство Росфинмониторинга № 12-2024 «О применении системы "Прозрачный блокчейн"» // Официальный сайт Федеральной службы по финансовому мониторингу. URL: <https://fedsfm.ru/documents/guide/12-2024>.
10. Бычков В. В., Вехов В. Б. Экспертиза при расследовании преступлений с криптовалютой // Криминалистический вестник. 2024. № 4. С. 67–73.
11. Долгиева М. М. Транснациональный характер криптовалютных преступлений // Журнал зарубежного законодательства. 2023. № 5.
12. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. М. : Ай Пи Ар Медиа, 2025.
13. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. 2023. № 4. С. 88–92.

14. Расследование преступлений, совершенных с использованием криптовалюты : учебное пособие / Д. А. Иванов, М. М. Макаренко, В. В. Пушкарев, Е. А. Русскевич. М. : Ай Пи Ар Медиа, 2021.

15. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий : учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А.А. Котова. М. : Изд-во Юридического института РУТ (МИИТ), 2025.

Терентьев А. А.¹,
старший преподаватель кафедры
инфокоммуникационных систем и технологий
Воронежского института МВД России,
кандидат технических наук

ПРИМЕНЕНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

С развитием информационных технологий и увеличением объемов передаваемых данных вопросы информационной безопасности становятся критически важными для организаций и частных пользователей.

В этом контексте актуальной задачей является обеспечение надежной защиты данных от несанкционированного доступа, утечек и других угроз. Одним из перспективных инструментов для моделирования и анализа систем безопасности являются сети Петри.

Сети Петри являются инструментом для моделирования и анализа дискретных событийных систем [1, с. 12]. Использование сетей Петри позволит создать модель для имитации защиты информации. В нашем случае сети Петри будут использоваться для описания процессов в области информационной безопасности.

Сеть Петри называется совокупность множеств [2, с. 94]

$$C_\mu = \{P, T, I, O, \mu\},$$

где: P – конечное множество, элементы которого называются позициями;

T – конечное множество, элементы которого называются переходами,
 $P \cap T = \emptyset$;

I – множество входных функций, $I: T \rightarrow P$;

O – множество выходных функций, $O: T \rightarrow P$;

μ – целочисленный вектор, $\mu = (\mu_1, \mu_2, \dots, \mu_n)$, $n = |P|$, $\mu_i = \mu(P_i)$, $i = \overline{1 \dots n}$.

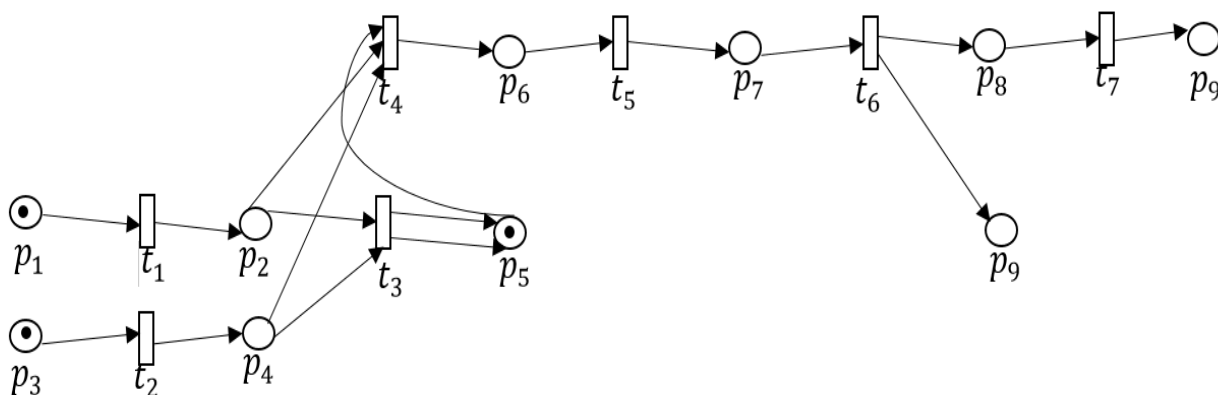


Рис. 1. Начальное состояние сети Петри

¹ © Терентьев А. А., 2025.

Позиции:

1. p_1 – *пользователь не авторизован* – начальное состояние, в котором пользователь не прошел аутентификацию.
2. p_2 – *пользователь авторизован* – пользователь успешно прошел проверку и получил доступ к ресурсам.
3. p_3 – *данные зашифрованы* – состояние, в котором данные находятся в зашифрованной форме для защиты от несанкционированного доступа.
4. p_4 – *данные расшифрованы* – данные доступны в открытом виде для авторизованных пользователей.
5. p_5 – *запрос на доступ* – представляет состояние, когда запрашивается доступ к данным или ресурсам.
6. p_6 – *обнаружена атака* – состояние, в котором система зафиксировала потенциально вредоносную активность.
7. p_7 – *блокировка доступа* – активное состояние предотвращения дальнейшего доступа после обнаружения угроз или аномалий.
8. p_8 – *обновление системы* – представляет процесс применения обновлений и исправлений для предотвращения известных уязвимостей.
9. p_9 – *завершение сессии* – состояние, представляющее завершение сеанса пользователя.

Переход:

1. t_1 – происходит аутентификация пользователя. Переход из состояния p_1 в состояние p_2 .
2. t_2 – происходит процесс шифрования в системе. Переход из состояния p_3 в состояние p_4 .
3. t_3 – осуществляется процесс запроса доступа после успешной аутентификации. Переход из состояния p_2 в состояние p_5 .
4. t_4 – происходит обнаружение атаки в системе. Переход может быть осуществлен сразу из нескольких состояний в одно, а именно переход осуществляется из состояний p_2 , p_4 и p_5 в p_6 .
5. t_5 – происходит блокировка, после обнаруженной атаки. Переход из p_6 в p_7 .
6. t_6 – происходит процесс завершения. Переход может осуществляться в два состояния из p_7 в p_8 и p_9 .
7. t_7 – происходит процесс завершения, как дополнительный переход при последовательном срабатывании таких процессов как обновление и завершение системы. Переход из p_8 в p_9 .

При построении сети Петри были использованы фишки на позициях, которые позволяют определить начальные и конечные состояния системы. А также при помощи фишек можно проанализировать работу системы. Исходя из *рис. 1–2* можно увидеть, что фишки стоят на позициях p_1 , p_3 и p_5 . Таким образом если сработает аутентификация, то фишка осуществит переход из состояния p_1 в состояние p_2 , через t_1 , и то же самое работает с переходом из состояния p_3 в состояние p_4 , через t_2 , при расшифровывании системы, то работа продолжится и до-

стигнет конечного состояния в позиции p_9 . Если же этого не случится, то сработает запрос на доступ и начальное состояние будет осуществляться за счет $p_5 \rightarrow t_4 \rightarrow p_6$ и до конечного состояния p_9 . Что же касается конечного состояния системы (p_9), то оно может быть достигнуто посредством двух путей, на прямую осуществляя завершение сессии или после обновления системы $p_8 \rightarrow t_7 \rightarrow p_9$.

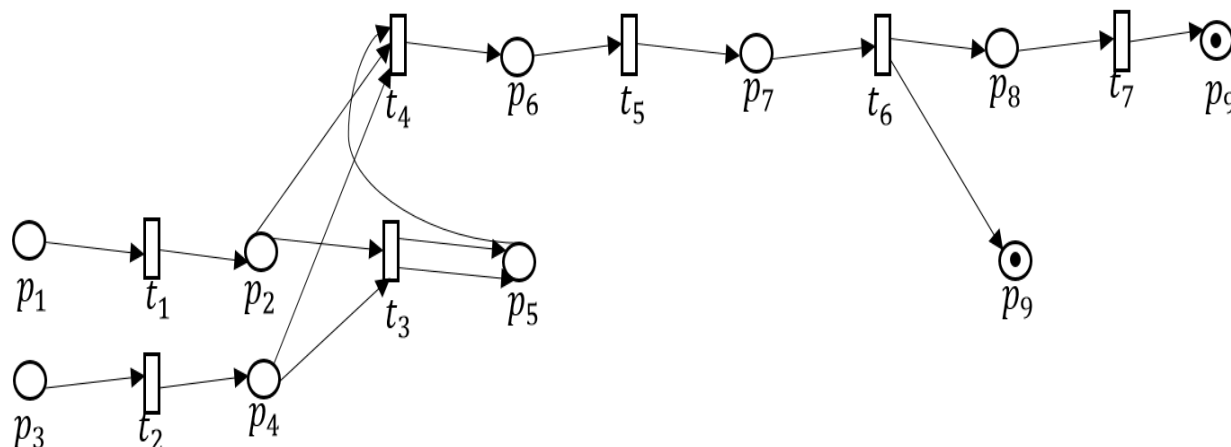


Рис. 2. Конечное требуемое состояние сети Петри

В заключение следует отметить, что сети Петри представляют собой мощный инструмент для моделирования и анализа сложных динамических систем, включая системы обеспечения информационной безопасности. Благодаря своей способности визуализировать и моделировать параллельные процессы и конкурентные события, сети Петри обеспечивают глубокое понимание потоков информации и потенциальных уязвимостей, что критически важно для разработки защищенных информационных систем.

Список литературы

1. Котов В. Е. Сети Петри. М. : Наука, 1984.
2. Терентьев А. А. Математическая модель аналитической деятельности ситуационных центров органов внутренних дел // Вестник Воронежского института ФСИН России. 2020. № 3. С. 91–97.
- 3.

Токолов А. В.¹,
доцент кафедры противодействия
преступлениям в сфере информационно-
телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук

МЕРЫ ПРЕДУПРЕДИТЕЛЬНОГО ХАРАКТЕРА, ПРИМЕНЯЕМЫЕ ОРГАНАМИ ПРАВОПОРЯДКА, В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Актуальность исследования предупредительных мер, принимаемых органами правопорядка, по обеспечению кибербезопасности приобретает особое значение ввиду увеличения количества преступлений, совершаемые посредством сети Интернет. Об этом свидетельствует увеличение правонарушений в 2021 г. было совершено 300337 киберпреступлений, в 2022 г. – 351463, т. е. на +17%, в 2023г. – 381112, на 9 8,4 % [16].

Особую опасность представляют социальные сети, в которых граждане выкладывают свои персональные данные, а также ежедневно общаются с неограниченным числом лиц, в том числе и преступниками. Доступность социальных сетей является криминогенным фактором, способствующим совершению преступления в киберпространстве. При этом по данным статистики аудитория социальных сетей постоянно растет. Например, в начале 2023 г. ежемесячная аудитория Telegram составила – 700 млн пользователей в месяц, а ВКонтakte – 79,5 млн пользователей [17].

Анализируя судебную статистику о киберпреступлениях, совершаемых в социальных сетях, следует указать, что в большей степени совершаются: мошенничества, незаконный оборот наркотических средств и их аналогов, а также оружия, призыв к совершению экстремистских преступлений в социальных сетях. Например, П.А.С. создал группу в социальной сети Telegram через группу DR.TIKKI, в которой продавался «МЕЛ». Фактически был создан интернет-магазин, посредством которого осуществлялся коммерческий сбыт наркотиков. Оплата наркотиков принималась в криптовалюте, а его получение посредством информирования покупателя о месте, где находится тайник-закладка. Таким образом, для осуществления сбыта наркотических средств использовалась социальная сеть «Telegram» [6].

Правоведы и специалисты по противодействию киберпреступлениям обращают внимание, что в целях обеспечения кибербезопасности в социальных сетях используются меры по обеспечению информационной безопасности личности, общества и государства. Например, государство возложило на себя обязанность по обеспечению информационной безопасности, основные положения которой

¹ © Токолов А. В., 2025.

нашли отражение в Указе Президента Российской Федерации № 646 [2], где указываются наиболее актуальные национальные интересы в информационной сфере, существующие информационные угрозы, а также определены стратегические цели, направления обеспечения информационной безопасности. В соответствии с п. «г» ч. 2 Указа Президента Российской Федерации № 646 обеспечение информационной безопасности представляет собой использование комплекса мер, направленных на прогнозирование, обнаружение, сдерживание, предотвращение, отражение информационных угроз, а также ликвидация их последствий. В рамках предотвращения реализации информационных угроз также используется правовой метод в форме привлечения лица к ответственности за совершение правонарушений в киберпространстве. С данной позиции предупредительные меры, используемые государством для предупреждения киберпреступлений, должны быть направлены на предотвращение киберугроз.

В литературе обращается внимание на необходимость толкования угроз информационной безопасности в качестве киберугроз, которые представляют собой наиболее опасное противоправное явление, так как злоумышленник имеет возможность совершить преступление удаленно и анонимно. Опытный программист и хакер способен скрыть свой цифровой след, вследствие чего правоохранительные органы не смогут не только найти преступника, но также и понять схему преступления, пресечь и предотвратить ее.

В правовой литературе под киберугрозами понимаются:

- распространение вредоносной информации, программ, алгоритмов и спама посредством сети Интернет, ставящие под угрозу персональную, общественную и государственную безопасность [5, с. 59]. Данный подход к определению понятия «киберугроза» является широким и понимает любые действия злоумышленника, которые посягают на информационную безопасность в целом;

- действия, совершаемые в виртуальном пространстве и посягающие на целостность, конфиденциальность и доступности компьютерных систем [11, с. 37]. С данной позиции киберугрозы направлены не на информационную безопасность конкретных лиц или структур, а посягают именно на компьютерные системы.

Объединяя два представленных подхода, следует указать, что под киберугрозами следует понимать действия по распространению вредоносной информации, программ алгоритмов и спама, посягающие на целостность, конфиденциальность и доступность компьютерных систем, создающие угрозы для персональной, общественной и государственной безопасности.

В целях обеспечения кибербезопасности, в том числе и в социальных сетях, в 2022 г. Указом Президента Российской Федерации было создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (далее – УБК) [3].

Деятельность УБК регламентируется приказом МВД России от 29.12.2022 г. № 1110, в котором определяются меры предупреждения киберпреступности [4], в том числе и совершаемых в социальных сетях.

Анализируя меры предупреждения киберпреступности в социальных сетях, применяемые УБК, необходимо выявить следующие:

- проведение мониторинга социальных сетей в целях выявления киберугроз и факта совершения киберпреступления. Данный мониторинг осуществляется посредством сбора, обобщения и анализа материалов, опубликованных в социальных сетях;
- проведение информационно-просветительской работы с населением в целях обеспечения кибербезопасности в социальных сетях;
- проведение оперативно-розыскных работ в целях выявления киберпреступлений в социальных сетях, в том числе и посредством участия в проведении мероприятий по получению доступа, съема и фиксации информации, содержащейся на электронных носителях и в информационно-телекоммуникационных сетях.

Анализ использования вышеуказанных мер противодействий, используемых для обеспечения кибербезопасности силами и средствами УБК указывает на их догматический, нежели практический характер. Это обусловлено тем, что сам термин «мониторинг социальных сетей» или «мониторинг информационно-телекоммуникационных сетей» не раскрывается в ФЗ «Об оперативно-розыскной деятельности».

А. В. Кутузов отмечает, что правоохранный мониторинг, который используется в целях противодействия киберпреступности в социальных сетях, выступает в качестве формы оперативно-розыскной деятельности, в том случае, если направлен на «поиск и фиксацию фактических данных по использованию информационных ресурсов в деструктивных целях; установление и изобличение субъектов этих действий для дальнейшего привлечения их к юридической ответственности и предотвращение деструктивной деятельности путем прекращения таких возможностей» [14].

С криминологической позиции в процессе использования правоохранный мониторинг необходимо использовать актуальные алгоритмы сбора, обработки и анализа данных в социальных сетях. Например, специалисты отмечают, что для выявления киберугроз в социальных сетях необходимо использовать анализ социальных граф. Данный подход позволяет исследовать группы, публикации и персональную информацию о пользователях для определения взаимоотношений между ними и выявление наличия связей между ними в целях установления киберугрозы для личной, общественной или государственной безопасности. Анализ социальных граф используется для выявления факта применения методов социальной инженерии. Например, отмечается, что данный подход направлен на «использование средств лингвистического и мультимодального анализа информации», который используется в социальных сетях в целях совершения киберпреступления [12].

В настоящее время основные направления мониторинга социальных сетей включают в себя изучение профилей пользователей, анализ их действий, определение групп и сообществ, связанных с преступными действиями, и дополнительный анализ основных слов и фраз. В результате мониторинга социальных сетей выявляются преступления, совершаемые посредством социальных сетей.

Однако мониторинг социальных сетей используется в целях предотвращения террористических и экстремистских преступлений. Выявление мошенничества

или незаконный оборот наркотиков осуществляется посредством принятия заявления от потерпевшего или посредством проведения просветительской работы с гражданами. Данные меры противодействия направлены, в большей степени, на расследование преступления и привлечения лица к ответственности, нежели на противодействие преступности. Например, в полицию обратились граждане, пострадавшие от мошеннических действий Л., который использовал группу ВКонтакте, где публиковались данные о продаже запчастей для зарубежных автомобилей. Л. под псевдонимом «А», используя VPN, публиковал в группе заведомо ложную информацию о наличии у него запчастей для автомобиля. Потенциальным клиентам Л. предлагал зарезервировать запчасти, перечислив аванс в размере 30 % от ее стоимости. После того, как деньги перечислялись на Qiwi кошелек, Л. блокировал «покупателя» и похищал денежные средства, принадлежащие ему. Таким образом, следствием было выявлено более 20 эпизодов мошеннических действий, совершенных посредством социальной сети ВКонтакте [7]. Однако данные преступления были выявлены не в результате проведения мониторинга социальных сетей, а обращения в полицию потерпевших.

Другим способом противодействия киберпреступности является проведение просветительской работы с гражданами, которое реализуется в двух направлениях:

- публикация в сети Интернет информации о способах противодействия преступлениям в социальных сетях, вариантах использования социальной инженерии и т. п. [15];
- проведение бесед с гражданами о распространенных методах мошенничества в сети Интернет [10].

В целях совершенствования обеспечения кибербезопасности в социальных сетях необходимо использовать более обширный перечень и спектр мер по их противодействию силами и средствами правоохранительных органов. Например, необходимо создать чат-бот в Телеграмм, куда может обратиться любое лицо, которому известна информация о киберугрозах.

Таким образом, правоохранительные органы осуществляют деятельность по противодействию киберпреступлениям в социальных сетях посредством использования правоохранительного мониторинга, проведения оперативно-розыскных мероприятий и информирования граждан о методах и способах обеспечения кибербезопасности.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) // СПС «КонсультантПлюс».
2. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».
3. Указ Президента Российской Федерации от 30.09.2022 № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» // СПС «КонсультантПлюс».

4. Приказ МВД России от 29.12.2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

5. Шпырна Е. Г. Современные тренды киберугроз / Е. Г. Шпырна, С. В. Световая // Международный студенческий научный вестник. 2024. № 6.

6. Приговор Октябрьского районного суда г. Киров от 13 февраля 2020 г. по делу № 1-44/2020 // URL: <https://sudact.ru/regular/doc/QfdjN3V9rHbV/>.

7. Приговор Щадринского районного суда Курганской области от 22 марта 2021 г. по делу № 1-490/2020 // URL: <https://sudact.ru/regular/doc/NECTAxgHrBW>.

8. Гнутова О. В. Анализ атак в информационной безопасности / О. В. Гнутова, Н. С. Мотуз // StudNet. 2022. Т. 5. № 1.

9. Kofman G. L. Cybersecurity issues in digital substations / G. L. Kofman, Yu. V. Piskovatsky // 24–26 апреля 2024 года, 2024. Р. 471–473.

10. Во Владикавказе сотрудники полиции провели с учителями школ и воспитателями детских садов беседы о распространенных методах мошенничества // URL: <https://xn--b1aew.xn--plai/news/item/23891275/>.

11. Алекперов И. Д., Горбачева А. А. Типы угроз кибербезопасности и способы борьбы с хакерством // Интеллектуальные ресурсы – региональному развитию. 2021. № 2. С. 37.

12. Босараб М. А., Иванов И. П., Колесников А. В. и др. Обнаружение противоправной деятельности в киберпространстве на основе анализа социальных сетей: алгоритм, методы и средства (обзор) // Вопросы кибербезопасности. 2016. № 4. С. 11–13.

13. Карцхия А. А., Макаренко Г. И., Сергин М. Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31).

14. Кутузов А. В. Оперативно-розыскной мониторинг сети Интернет как элемент противодействия преступлениям экстремистской направленности // Вестник Костромского государственного университета. 2020. Т. 26. № 2. С. 235–241.

15. Памятка для граждан о профилактике и предупреждении дистанционных преступлений // URL: <https://xn--80aafwghfew0e.34.xn--b1aew.xn--plai/news/item/31056223/>.

16. Статистика и аналитика МВД России // URL: <https://мвд.рф/dejatelnost/statistics>.

17. Статистика социальных сетей // URL: <https://inclient.ru/vk-stats/>.

18. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. М. : Ай Пи Ар Медиа, 2025.

19. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : сборник научных трудов Международной научно-практической конференции. М. : Московский университет МВД России имени В.Я. Кикотя, 2024. С. 35–37.

20. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. 2024. № 5. С. 149–155.

21. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий : учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова. М. : Изд-во Юридического института РУТ (МИИТ), 2025.

Трофимов В. Е.¹,
*доцент кафедры противодействия
преступлениям в сфере информационно-
телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ПРЕДУПРЕЖДЕНИЕ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ОБОРОТА ЦИФРОВОЙ ВАЛЮТЫ

Современное российское общество в настоящее время продолжает динамично развиваться, используя для этого различные доступные инструменты, в том числе достижения науки и техники.

Российская Федерация выступает одним из активных участников мировой экономической системы, в которой получили широкое распространение цифровые финансы. В связи с этим, государства стремятся урегулировать возникающие с участием цифровых финансов правоотношения, адаптируя для этого экономический сектор. Так, Президент США Дональд Трамп заявил о необходимости создания в стране стратегического резерва цифровых активов. Кроме того, осуществлен выпуск такого актива с названием «TRUMP», а также существуют и другие цифровые активы членов его семьи.

При этом представляет острую необходимость разработка нормативной правовой основы для организации оборота такого рода финансов. Уместно отметить, что России в 2020 г. вступил в силу федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», который наряду с устранением имеющихся понятийных пробелов установил порядок осуществления майнинга. Кроме того, внесенные изменения указывают, что цифровая валюта для целей Федерального закона от 25.12.2008 № 273 «О противодействии коррупции» признается имуществом.

Действующее в России законодательство ввело в оборот термин «цифровая валюта» и не содержит понятия «криптовалюта», которое сформировалось под влиянием применяющейся при ее создании технологии криптографии. Особенностью выступает публичность осуществляемых транзакций криптовалюты, которые находят свое отражение в реестре данных операций, формируемом на основе технологии распределительного реестра (блокчейн) [1, с. 86].

Для функционирования исследуемого финансового сектора не требуется какого-либо центра управления или общего сервера для хранения информации, так как она распределена между множеством узлов различных пользователей. Каждый такой блок содержит уникальный код, изменить который невозможно.

¹ © Трофимов В. Е., 2025.

Именно отсутствие возможности влияния на оборот цифровой валюты (криптовалюты) со стороны банковской системы и государств в целом, популяризует ее использование по всему миру.

Наряду с указанным преимуществом цифровой валюты над традиционной финансовой системой еще одним достоинством криптовалюты выступает анонимность использования. Для осуществления транзакций с ее участием не требуется подтверждение личности или какие-либо данные, кроме адреса кошелька получателя, куда происходит отправление.

Высокая скорость транзакций цифровой валюты независимо от объема и расстояния также представляет собой определенное преимущество в сравнении с классическим банковским сектором.

Немаловажным фактором выступают и низкие комиссии за переводы. При этом различные компании осуществляют постоянную работу по улучшению условий использования именно их продукта, снижая комиссии и скорость транзакций.

Одним из важнейших факторов, способствующим распространению цифровых финансов по всему миру является доступность пользователей к финансовым инструментам. Независимо от местонахождения и наличия банковской системы пользователи могут принимать участие в мировой финансовой системе.

Развитие цифровой валюты способствовало созданию специальных бирж, где происходят различные операции с применением классических финансовых инструментов.

Уместно обратить внимание, что особенный интерес проявляется к децентрализованному сектору.

Популярность криптовалюты во всем мире, в том числе в России, подталкивает все больше лиц совершать различные виды сделок с ней. Данное обстоятельство порождает в свою очередь повышенное внимание к цифровым финансам со стороны преступности.

Одним из наиболее распространенных преступлений в данной сфере является мошенничество.

Среди способов совершения мошенничества следует назвать наиболее популярные.

Схема «треугольник» является одним из самых распространенных в мире способов совершения преступлений, причем не только в сфере криптовалюты.

Суть указанного способа заключается в том, что преступник своими действиями организует взаимодействие двух законопослушных, ничего не подозревающих лиц, желающих совершить законные действия.

В качестве примера следует привести ситуацию, когда потенциальный преступник создает объявление о продаже своего имущества по привлекательной, заниженной цене, желая осуществить сделку удаленно (отправить почтой и т. п.). Найдя покупателя, злоумышленник открывает P2P сделку на криптовалютной бирже, где ничего не подозревающий участник криптовалютного рынка предоставляет для денежного перевода реквизиты банковской карты, после чего планирует отправить заранее определенное количество цифровых финансов. При этом преступник указывает полученные им от участника криптовалютного

рынка реквизиты банковской карты как свои, для перечисления оплаты за продаваемое им имущество. Далее, участник P2P сделки получает на свою банковскую карту денежные средства от покупателя имущества, а определенное количество криптовалюты отправляет преступнику. В результате потенциальный покупатель перевел денежные средства не за планируемую им покупку, а за криптовалюту, при этом обращение в правоохранительные органы происходит на продавца криптовалюты, так как именно его реквизиты банковской карты были указаны.

В качестве профилактики подобных ситуаций, чтобы не стать жертвой подобных действий, необходимо соблюдать некоторые правила предосторожности:

- совершать сделки в P2P секторе с наиболее опытными продавцами, имеющими, например, 100 и более успешных сделок;
- знакомиться с отзывами о продавце цифровых финансов;
- не участвовать в сделках с банковскими картами третьих лиц;
- взаимодействовать со службой поддержки и т. п.

Следующим способом мошеннических действий в сфере цифровых финансов является предоставление недобросовестных обучающих услуг в данной сфере. Например, обучая работе с криптовалютными кошельками, потенциальный преступник заявляет о необходимости предварительно приобрести определенное количество цифрового актива, в чем предлагает свою помощь. Жертва переводит денежные средства нарушителю для приобретения криптовалюты, однако получив деньги, злоумышленник пропадает. Кроме того, нередки случаи, когда преступники, получив доступ к криптовалютному кошельку обучающегося, похищают находящиеся на нем активы.

В качестве профилактики совершения подобных действий необходимо также внимательно знакомиться с организацией, занимающейся предоставлением подобного рода обучающих услуг, не сообщать информацию третьим лицам, позволяющую распоряжаться вашими активами, хранить имеющиеся цифровые финансы на различных кошельках.

Особого внимания заслуживает существующий также много лет способ получения конфиденциальных данных пользователей посредством фишинговых сайтов. В мире как централизованных, так и децентрализованных финансов данный способ остается популярным. Преступники создают сайт с доменным именем, схожим с популярным в криптовалютном мире ресурсом, где обманутые пользователи либо вводят необходимые злоумышленникам данные, либо начинают хранить свои активы, которые в последствие пропадают.

Чтобы не стать жертвой фишинговых сайтов необходимо тщательно проверять наименование в адресной строке, использовать антивирусные программы на своем устройстве, не переходить по коротким ссылкам, даже если они приходят от знакомых, использовать браузеры с антифишинговой защитой, сохранять в избранное адреса сайтов, которые наиболее часто используются для работы с различными финансовыми инструментами.

Вместе с тем указанные выше способы совершения преступлений присущи не только сфере цифровых финансов, в связи с чем необходимо обратить внимание на те противоправные деяния, которые чаще встречаются именно в исследуемой сфере.

Так, одним из популярных способов среди преступного элемента является создание телеграмм-каналов, которые специализируются на привлечении аудитории обещаниями преумножить их денежные средства за счет спекуляций на различных криптовалютных инструментах. В данном случае жертвы преступлений переводят деньги в доверительное управление потенциальным преступникам и ждут прибыли.

Рассмотренные способы совершения преступлений лишь часть среди тех, которые применяются субъектами преступлений. При этом преступность изобретает новые возможности похитить имущество у населения. В такой ситуации правоохранительные органы должны актуализировать способы противодействия указанной негативной тенденции. Названные профилактические рекомендации носят общий характер и на системной основе подлежат совершенствованию и дополнению.

Необходимо отметить, что основной профилактической мерой на современном этапе развития сферы цифровых финансов может выступить полноценное законодательное регулирование названной отрасли. В частности, подробная правовая регламентация позволит создать условия для появления юридических лиц, оказывающих различные услуги в сфере цифровых финансов, доступность которых способствует снижению преступности в исследуемой сфере, так как население сможет взаимодействовать с проверенными структурами [2, с. 127].

Список литературы

1. Пинкевич Т. В. Предупреждение преступлений, совершаемых в сфере оборота цифровой валюты (криптовалюты) // Правовое государство: теория и практика. 2021. № 4 (66). С. 82–96.
2. Зайнутдинова Е. В. Цифровые права и цифровая валюта: сравнительно-правовое исследование // Журнал зарубежного законодательства и сравнительного правоведения. 2024. Т. 20, № 1. С. 117–129.
3. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. 2024. № 5. С. 149–155.
4. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. М. : Московский университет МВД России имени В.Я. Кикотя, 2024. С. 35–37.
5. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. М. : Ай Пи Ар Медиа, 2025.

6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. М. : Ай Пи Ар Медиа, 2025.

7. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. Саратов : М. : Профобразование : Ай Пи Ар Медиа, 2025.

8. Расследование преступлений, совершенных с использованием криптовалюты : учебное пособие / Д. А. Иванов, М. М. Макаренко, В. В. Пушкарёв, Е. А. Рускевич. М. : Ай Пи Ар Медиа, 2021.

Фокин А. Д.¹,
*ассистент кафедры криминалистики
Московского государственного юридического
университета имени О. Е. Кутафина (МГЮА)*

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ

Следует констатировать, что современное мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий, наносит непоправимый вред обществу и государству. Негативные последствия данного криминального деяния оказывают деструктивное влияние на разные социальные и государственные институты. В том числе сказываются и на нормальной управленческой деятельности органов государственной власти. При совершении данного вида мошенничества, преступники часто выдают себя за сотрудников правоохранительных органов. Также злоумышленники используют современные специальные программы, подменяющие телефонные номера, в результате чего у абонента отображается входящий звонок с местных (региональных) телефонов сотрудников ФСБ РФ, СУ СК РФ или МВД России. При этом далеко не во всех случаях преступники высылают потерпевшим по средствам связи подложные удостоверения и иные документы (зачастую процессуальные), подтверждающие легитимность их статуса и действий. Как показало обобщение следственной практики по данным видам мошенничества, такие действия присутствовали лишь в 11 % случаев. В таких ситуациях действия мошенников требует дополнительной квалификации по ч. 1 ст. 327 УК РФ (Подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков).

В большинстве преступлений мошенники ограничивались устным заявлением в адрес жертв о наличии таких полномочий. Используя методы и приемы психологического воздействия, мошенники настолько убеждают потерпевших, что последние искренне верят, что действовали в рамках специальных операций правоохранительных органов (например, по поимке преступников). Также, как показали результаты интервьюирования сотрудников правоохранительных органов, в подавляющем большинстве случаев (87 %) мошенники действуют группой – звонят от имени представителей силовых ведомств, подтверждают слова друг друга, чтобы повысить уровень доверия у жертвы.

В условиях современного социума можно констатировать, что при общей стагнации общественного доверия к сотрудникам полиции, на фоне генезиса дистанционного мошенничества происходит укоренение негативных социальных стереотипов на фоне роста разрыва связей с населением. Как показали результаты нашего интервьюирования, из 70 опрошенных жителей г. Москвы 49 ассо-

¹ © Фокин А. Д., 2025.

цируют поступление звонков от правоохранительных органов с мошенническими действиями [1, с. 144], а 63 % респондентов отметили работу правоохранительных органов в данном направлении, как неэффективную.

Обозначенный аспект проблемы имеет и ряд частных ответвлений. Так, отдельного внимания заслуживает вопрос об эффективности использования на практике тактико-криминалистических рекомендаций, направленных на проведение следственных действий с участием потерпевших от данного вида преступлений лицами. Следует отметить, что особенности психологического состояния жертв, как результат действий телефонных мошенников, помимо традиционных факторов (совершение в отношении гражданина преступного деяния, вовлечение его в сферу уголовного судопроизводства), обуславливаются рядом дополнительных детерминантов и должны учитываться в процессе организации и проведения следственных действий с их участием.

Во-первых, поскольку ряд способов мошенничества может повлечь утрату потерпевшими прав на единственное жилье в совокупности с потерей значительной суммы денег (ч. 4 ст. 159 УК РФ), они испытывают сильное эмоциональное потрясение, порой затрудняющее получение объективных показаний, особенно на первоначальном этапе расследования. Показания потерпевших, находящихся в состоянии стресса, характеризуются эпизодичностью воспоминаний, замещением сведений об элементах события преступления, воспоминаниями самих эмоций, сопровождающих данное событие на разных его этапах. Исходя из этого, рекомендуется допрашивать таких лиц незамедлительно (в первые дни после возбуждения уголовного дела) и использовать тактические приемы, основанные на ассоциативных и эмоциональных связях, позволяющие потерпевшему вспомнить возникшие эмоции, сопутствующие отдельным обстоятельствам события преступления (момент встречи с мошенником, момент переговоров, оформления документов и т. д.) [2, с. 101].

Во-вторых, из-за того, что преступники используют психологические приемы манипулирования сознанием и поведением жертвы, последние порой не всегда адекватно понимают и интерпретируют характер и значение совершаемых в отношении них действий. Даже, находясь на допросе, они не всегда осознают, что с ними произошло. Так, в рамках одного уголовного дела была установлено, что мошенники, представившись сотрудниками правоохранительных органов и банковских организаций, путем дезинформации убедили жертву в реальности существования угрозы ее жизни и имущества. В результате, когда к потерпевшей пришли обеспокоенные родственники, она была так испугана, что приняла их за бандитов и хотела сбежать через окно. Находясь в тяжелом эмоциональном состоянии, в ходе предварительного следствия она с трудом давала показания, постоянно путалась в обстоятельствах происшедшего. Следует согласиться, что в таких ситуациях классические приемы получения и оценки информации, исходя из ее заведомо ложной или добросовестно искаженной природы, малоэффективны. Здесь приоритет должен отдаваться комплексному использованию специальных знаний из психологии, психофизиологии и смежных областей [3, с. 26].

В-третьих, необходимо учитывать, что некоторые из жертв на момент их допроса остаются вовлеченными в неприятные процессы, связанные с последствиями совершения в отношении них преступления (прохождение процедуры банкротства, оспаривание кредитной сделки и пр.).

В-четвертых, среди потерпевших встречаются лица, которые не просто понесли существенный материальный ущерб от мошеннических действий, но и под воздействием преступников пытались совершить противоправные действия. Находясь в таком состоянии в совокупности с возрастными характеристиками (как правило, люди пенсионного возраста), такие лица зачастую находятся в состоянии фрустрации. Испытывая чувства шока, вины и беспомощности поменять случившееся, они безразлично, а порой скептически относятся к деятельности правоохранительных органов. Усугубляется это тем, что мошенники при совершении преступлений представлялись сотрудниками правоохранительных органов.

Указанные психологические особенности предопределяют выбор тактических приемов, направленных на преодоление негативного эмоционального состояния потерпевших. Как показали наши исследования, у потерпевших по данной категории дел наблюдается эффект эмоционального накопления, когда негативные эмоции подавляются, но не исчезают, а аккумулируются в психике. В результате допрашиваемые постоянно испытывают чувство беспокойства, что приводит к быстрому их утомлению во время проведения следственных действий (особенно первоначальных) и потери концентрации внимания.

Сопутствующим негативным фактором, влияющим на эффективность коммуникации с такими лицами, является пересмотр ими своих базовых качеств, явившихся причиной обмана: склонность к доверию, поиск эмоциональной близости, желание быть полезным и пр. В связи с этим следователь должен строить тактику допроса, исходя из таких положений, как: проявление сочувствия, демонстрация спокойствия и терпимости, проявление внимания, сокращение дистанции общения, поддержание визуального контакта и пр.

На наш взгляд, в уголовно-правовом аспекте анализируемой проблемы законодателю можно пойти по пути ст. 210.1 УК РФ, введенной в целях ужесточения уголовной ответственности за создание преступного сообщества (преступной организации) и руководство таким сообществом (такой организацией). Следуя смыслу ст. 210.1 УК РФ для привлечения лица к уголовной ответственности необходимо, чтобы виновный занимал высшее положение в преступной иерархии и совершение таким лицом хотя бы одного умышленного действия (постановка задач, дача поручений и др.), направленного на координацию деятельности любой общности лиц, условившихся о совершении преступлений. Как свидетельствует практика, ст. 210.1 УК РФ оказалась востребованной. Она дала возможность привлечь к уголовной ответственности лидеров преступной среды во многих регионах страны.

Один из возможных путей выхода из ситуации – дополнить ст. 159 УК РФ соответствующим положением, ужесточающим ответственность за действия мошенников, выдаваемых себя за сотрудников правоохранительных органов. Подобный способ криминализации обусловлен, в первую очередь, сложностями в

процессе доказывания преступной деятельности телефонных мошенников. Последние не принимают непосредственное участие, например, в продаже жертвой недвижимого имущества, а лишь координируют такие действия, вводя собственника жилья в заблуждение. В результате потерпевший, не имея реальной возможности распознать истинные намерения мошенников, содействует преступникам. Обман для него становится очевидным уже после того, как жилье было реализовано. Формальная законность сделки и содействие потерпевшего в ее осуществлении, а также заверения мошенника о том, что другое жилье или деньги будут предоставлены потерпевшему в ближайшем будущем, не позволяют пострадавшему от мошеннических действий вовремя обратиться за помощью в правоохранительные органы. Что и обуславливает проблемный характер первоначальных ситуаций расследования.

Кроме того, необходимо учитывать, что использование преступниками, выдающими себя за сотрудников силовых структур, персонифицированных психологических приемов воздействия на потенциальных жертв, невозможно без использования ими персональных данных таких лиц. Следует констатировать, что в настоящее время сведения об имуществе, составе семьи, уровне дохода, документах и штрафах и пр. являются отдельным объектом посягательства преступников на стадии подготовки к обманному завладению имуществом граждан. Как отметил генеральный прокурор РФ И. Краснов, в 2024 г. в результате утечки персональных данных атаке телефонных мошенников подверглись более 110 тыс. лиц пенсионного возраста. В связи с этим предлагаемый нами путь криминализации действий мошенников, выдающих себя за сотрудников правоохранительных органов, должен сочетаться с ужесточением ответственности за умышленную массовую утечку персональных данных и одновременной унификацией массива нормативных правовых актов, регулирующих обработку персональных данных.

На наш взгляд, ч. 3 ст. 159 УК РФ можно изложить в следующей редакции: *«Мошенничество, совершенное лицом с использованием своего служебного положения, а равно путем выдачи себя за сотрудника правоохранительных органов, а также в крупном размере...»*. Отметим, что в предлагаемой нами редакции основание уголовной ответственности будет акцентироваться не на степени опасности личности (как в ст. 210.1 УК РФ), а на поведении и деятельности такого лица. Представляется, что такая ответственность должна наступать не только при наличии факта выдачи виновным лицом себя за сотрудника правоохранительных органов, но и совершения им умышленных действий (дача поручений и пр.), направленных на координацию действий лица, в отношении которого осуществляется хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Предлагаемая редакция позволит органам уголовного преследования при изобличении виновного использовать схему расследования и доказывания — от лица к преступлению. Если проводить аналогию со ст. 210.1 УК РФ, такой алгоритм является весьма эффективным и обусловлен спецификой данного ме-

ханизма криминального деяния. В частности, за период с 2020 г. по 2023 г. судами субъектов Российской Федерации по ст. 210.1 УК РФ осуждено 74 лица [4, с. 157].

Также представляется, что введение данного положения, как ответной меры государства на распространение телефонного мошенничества, требует, как это отметил В. В. Путин в ходе совещания с членами правительства, постоянного анализа правоприменительной практики и соответствующих корректировочных решений (и действий). Подобная корректировка должна касаться не только совершенствования юридической техники при формулировке любой новой нормы, но и проходить с учетом иных направлений борьбы с преступностью. В этом плане уголовно-правовые меры борьбы с телефонным мошенничеством должны усиливаться средствами (и технологиями) информационной борьбы с подобного рода криминальными деяниями. А именно:

- регулярное освещение в СМИ в виде программ, интервью с должностными лицами, публикаций, видеосюжетов, социальной рекламы вопросов профилактики и противодействия современным мошенническим схемам;
- внедрение в повседневную жизнь граждан цифровых приложений – памяток, в которых будет собрана информация о наиболее распространенных схемах мошенничества;
- формирование единого центра противодействия телефонному мошенничеству, объединяющего работу правоохранительных органов, банков, крупных операторов связи и владельцев интернет-ресурсов в целях оперативного обмена базами данных о фактах выявленных мошеннических действий и лиц, их совершивших;
- автоматизация процесса сбора, систематизации, обработки и анализа сведений о дистанционных преступлениях, совершенных с использованием информационно-телекоммуникационных технологий (на примере системы «Дистанционное мошенничество»).

Список литературы

1. Зуева О. В., Демидов Н. Н. Доверие граждан к полиции в современной России: актуальное состояние и анализ факторов // Вестник Московского государственного лингвистического университета. Общественные науки. 2022. № 2. С. 141–150.
2. Тактоева В. В. Тактические особенности проведения допроса специалиста и потерпевшего при расследовании уголовных дел о мошенничестве, совершенном в жилищной сфере // Криминалистика: вчера, сегодня, завтра. 2021. № 4. С. 97–105.
3. Комиссарова Я. В. Ложные воспоминания: проблемы оценки показаний участников уголовного судопроизводства // Российский судья. 2023. № 4. С. 22–28.
4. Бажутов С. А. Актуальные проблемы уголовной ответственности лиц, занимающих высшее положение в преступной иерархии (статья 210.1 УК РФ) // Правопорядок: история, теория, практика. 2024. № 3. С. 155–161.

Цурлуй О. Ю.¹,
*доцент департамента уголовного права,
процесса и криминалистики
НИУ «Высшая школа экономики»,
кандидат юридических наук, доцент*

РОЛЬ КРИМИНАЛИСТИЧЕСКОЙ ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Si gladius tuus brevis est, impetum cum scuto. – Если короток твой меч, атакуй щитом (лат.)

Криминалистическая профилактика переживала различные этапы в составе предмета криминалистики – от включения до полного исключения, что вполне объяснимо. Сложно представить криминалистическую профилактику грабежей и разбоев. Очевидно, что эффективность криминалистических методов и средств противодействия названным видам преступлений будет нулевой. Предупреждением краж, грабежей и разбоев должна заниматься криминология, исходя из условий, причин и личности субъектов указанных преступлений. И в этой связи нельзя не согласиться с утверждением Зайнуллина Р. И., что «криминалистическая профилактика – это иллюзорное, фантомное и мифичное учение» [3, с. 58], которое безусловно актуально для 80-х, 90-х и даже 00-х гг. Однако жизнь не стоит на месте, преступность совершенствуется, используя новые технологические и технические достижения. Криминалистика должна развиваться опережающими темпами, чтобы эффективно выполнять свою первоочередную задачу борьбы с преступностью.

Справедливо указывает Б. Б. Батров, «учитывая, что дистанционные мошенничества в большинстве своем совершаются с использованием IP-телефонии, при совершении которых имеющимися техническими средствами установить виновных лиц не представляется возможным, считаем необходимым для сокращения регистрации данного рода преступлений, вплоть до значительного уменьшения их количества, определить основную задачу – борьбу путем применения мер криминалистической профилактики» [1, с. 26].

Мошенничество с использованием цифровых технологий наиболее яркий пример того, что наука криминалистика должна разработать методы противоборства со способами преступлений, позволяющими совершать общественно опасные деяния и причинять вред гражданам и государству из-за рубежа. Прежние подходы к сущности и содержанию криминалистической профилактики в современной структуре преступности неэффективны.

Насущная необходимость пересмотра определения криминалистической профилактики коррелирует с положениями п. 11 ст. 47 Указа Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопас-

¹ © Цурлуй О. Ю., 2025.

ности Российской Федерации», согласно которым «достижение целей обеспечения государственной и общественной безопасности осуществляется путем реализации государственной политики, направленной на решение задач по предупреждению и пресечению правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют».

Наиболее подходящим, на наш взгляд, действием в основе криминалистической профилактики является противоборство, т. е. «борьба против кого-чего-нибудь» [9, с. 624], поскольку представляется наиболее активной деятельностью.

Обобщив изложенные в специальной литературе определения криминалистической профилактики, отметим, что данная деятельность, по мнению ученых, представляет собой «совокупность разработанных криминалистикой методов и средств, применяемых органами предварительного следствия и дознания по недопущению совершения преступлений путем выявления, устранения или нейтрализации причин, условий и обстоятельств, способствующих их совершению; оказанию профилактического воздействия на лиц с противоправным поведением, в том числе исключая возможность совершения преступлений» [2, с. 194; 8, с. 190; 9, с. 853; 12, с. 94; 4, с. 97–98; 13, с. 193; 14, с. 207].

Согласимся с мнением О. В. Полстоваловым, что «профилактика должна быть реализована как можно раньше. Плотная увязка криминалистической профилактики с уголовно-юрисдикционной деятельностью изжила себя и требует пересмотра в сторону профилактики предкриминальных явлений» [11, с. 308].

Полагаем, что на современном этапе роль криминалистической профилактики состоит в противоборстве способу совершения преступления, путем его нейтрализации либо существенного затруднения его реализации.

Преступность, как «сложное, многоаспектное негативное социальное явление, исследуется криминалистикой, прежде всего, с функциональной его стороны, системы действий и взаимосвязей, образующих способ, механизм преступления и его следовое отражение в окружающей обстановке» [6, с. 7].

Советский криминалист Г. Ю. Маннс называл способы совершения преступлений важнейшим элементом предмета науки криминалистики. Именно «способ совершения преступления является важным признаком любого преступления» [3, с. 102].

Криминалистика определяет способ совершения преступления как «систему действий, направленных на предварительную подготовку, непосредственное совершение и посткриминальное сокрытие преступлений» [3, с. 105].

Посредством анализа способов совершения преступлений, «можно вычислить преступную среду, различные уловки преступников и косвенно использовать знания об этом в целях профилактики преступлений» [15, с. 7].

Очевидными примерами эффективной криминалистической профилактики посредством воздействия техническими мерами на способ совершения преступления выступает деятельность банковского сектора и мобильных операторов.

Криминалистическая профилактика, воздействующая на способ совершения преступлений, приобрела эффективность в то время, когда структура преступности не позволяет фактическое задержание и привлечение лиц, совершающих преступление к уголовной ответственности. Обусловлена такая ситуация технологическими возможностями и международной обстановкой, когда лица, совершающие, например, «телефонные мошенничества», физически находятся за пределами нашей страны.

Разработанные операторами сотовой связи антифрод системы являются эффективным методом криминалистической профилактики, поскольку существенно затрудняют его реализацию. Так, например, мобильный оператор Билайн признан самым безопасным среди крупнейших операторов России по защите абонентов от мошенничества, спама и распространения нелегальных (серых) SIM-карт. Это подтверждается результатами исследования, проведенного аналитиками ComNewsResearch.

Еще одним примером существенного снижения преступлений конкретного вида является введение видеофиксации нарушений правил участниками дорожного движения. Автоматизация процесса нарушений водителями правил дорожного движения от момента фиксации до оформления постановления об административном правонарушении и назначения административного наказания существенно снизило уровень взяточничества среди сотрудников Госавтоинспекции. Видеофиксация, в том числе использование видеорегистраторов, позволяет проследить фактические обстоятельства происшествия, обосновать каждым участником объективность своей позиции и повышает эффективность борьбы с данным видом преступлений в целом.

Стоит также отметить, что данный пример является показателем эффективного применения в комплексе технических и законодательных мер.

Противоборство реализации способа совершения преступления путем ее затруднения, снижением экономической выгоды влечет фактическое снижение числа преступлений, совершаемых таким способом, что свидетельствует об эффективности криминалистической профилактики по принципу, если короток меч, бей щитом.

Не вызывает сомнения, что изменение определения криминалистической профилактики расширяет перечень субъектов профилактической деятельности в рамках борьбы с преступностью. Ученые-криминалисты являются субъектами криминалистической профилактики. Именно в наши задачи входит разработка эффективных и действенных профилактических мер, затрудняющих совершение новых преступлений, противодействия существующим способам совершения преступления, расследование которых и объективно затруднено.

В свою очередь решение этих задач «способствует формированию и совершенствованию научного аппарата криминалистики (понятий, принципов, классификаций, общей и частной теории, учений, и т. д.)» [7, с. 6].

В заключение отметим, что чем ближе криминалистическая профилактика к лицу, совершающему преступление, тем она активнее и эффективнее, и носит наступательный характер, противоборствует непосредственно способу соверше-

ния преступления и лицу, его совершающему. Криминалистическая профилактика, воздействующая на потенциального потерпевшего от преступного посягательства, носит именно защищающий характер, противопоставляя способу совершения преступления опосредовано, через разъяснение его лицу, в отношении которого направлено общественно опасное деяние.

Список литературы

1. Батров Б. Б. Криминалистическая профилактика интернет-мошенничеств: проблемы раскрытия и расследования // Вестник Бурятского государственного университета. Юриспруденция. 2021. № 1. С. 21–28.
2. Бессонов А. А. Основные теоретические положения криминалистической профилактики // Расследование преступлений: проблемы и пути их решения. 2017. № 2 (16). С. 148–154.
3. Григорян Д. К. Криминалистическое учение о способе совершения преступления в контексте формирования системы способов совершения элитарных преступлений // Юристъ-Правоведъ. 2023. № 4 (107). С. 102–106.
4. Зайнуллин Р. И. Криминалистическая профилактика – миф или реальность? // Криминалистика. 2023. № 4 (45). С. 53–56.
5. Коломинов В. В. Криминалистическая профилактика преступлений экстремистской направленности, совершенных с помощью современных технологий // Сибирский юридический вестник. 2023. № 2 (101). С. 92–100.
6. Криминалистика : учебник для бакалавров и специалистов / отв. ред. д.ю.н., проф. Е. П. Ищенко. М.: Проспект, 2020.
7. Криминалистика : учебник / отв. ред. Н. П. Яблоков. 2-е изд., перераб. и доп. М. : Юристъ, 2001.
8. Лантух Э. В. Сущность и значение криминалистической профилактики // Научные труды Северо-Западного института управления РАНХиГС. 2016. Т. 7. № 1 (23). С. 190–194.
9. Меретуков Г. М., Лунина Е. С., Бирюкова С. Н. Криминалистическая профилактика по конкретному уголовному делу о незаконном обороте наркотиков // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2017. № 128. С. 837–854.
10. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В.В. Виноградова. 4-е издание., дополненное. М. : Азбуковник, 1997.
11. Полстовалов О. В. Цифровизация и криминалистическая профилактика преступлений // Правовые проблемы укрепления российской государственности: Сборник статей Всероссийской научно-практической конференции, Томск, 28–30 января 2021 года. Часть 89. Томск : Национальный исследовательский Томский государственный университет, 2021. С. 307–309.
12. Топорков А. А. Криминалистическая методика расследования преступлений : учебник. М. : Юстиция, 2018.

13. Шалкарова Ким И. А. Криминалистическая профилактика преступлений // Вестник Казахского национального университета. Серия юридическая. 2018. Т. 87. № 3. С. 189–194.
14. Шруб М. П. Криминалистическая профилактика как элемент общеправовой системы мер предупреждения преступности // Вестник Полоцкого государственного университета. Серия Д. Экономические и юридические науки. 2017. № 6. С. 206–210.
15. Якимов И. Н. Криминалистика. Руководство по уголовной технике и тактике. М., 1925.

Чехович А. А.¹,

адъюнкт научно-педагогического факультета

Академии Министерства внутренних дел Республики Беларусь

ЛИЧНОСТЬ ПРЕСТУПНИКА, КАК ЭЛЕМЕНТ ОПЕРАТИВНО-РОЗЫСКНОЙ ХАРАКТЕРИСТИКИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Современные условия развития мировой цивилизации характеризуются нарастанием и ускорением процессов глобализации, которые несут определенные блага и в то же время служат идеальной основой для трансформации существующих и появлению принципиально новых угроз безопасности как отдельным государствам, так и всего мирового сообщества в целом. Руководствуясь корыстными и иными деструктивными мотивами, используя информационное пространство сети Интернет для совершения противоправных действий, преступники совершают различные преступления, в том числе и несанкционированный доступ к компьютерной информации (далее – НДКИ), ответственность за который предусмотрена ст. 349 Уголовного кодекса Республики Беларусь.

Преступление как объект познания рассматривается различными науками по-разному. Поэтому существуют различные характеристики преступлений: криминалистическая, уголовно-правовая, криминологическая, виктимологическая, нравственно-психологическая, социальная. Для оперативно-розыскной науки, учеными, для описания свойств отдельных видов и форм преступлений разработана оперативно-розыскная характеристика (ОРХ) [1, с. 70]. ОРХ является теоретической информационной моделью преступления, отражающей взаимосвязь ее элементов, для выбора наиболее оптимального варианта использования оперативно розыскных сил, средств и методов для наиболее качественного и быстрого раскрытия подготавливаемого или совершенного преступления.

По мнению А. М. Абрамова, ОРХ представляет собой систему свойств и информационных признаков, присущих определенному виду преступлений, знание которых способствует эффективному решению организационно-тактических задач по их предупреждению и раскрытию, а также служит теоретической и информационной основой для разработки тактических приемов с целью эффективного раскрытия конкретных преступлений [1, с. 83]. В свою очередь, И. И. Басецкий определяет ОРХ как совокупность гласной и негласной информации о распространенности этого вида преступлений в республике, их характере, особенностях проявления [2]. В настоящее время ОРХ НДКИ еще не разработана. Тем не менее в отдельных публикациях криминалистической характеристики НДКИ фрагментарно указываются элементы, которые могут использоваться при ее построении [3, 4].

Рассматривая содержание ОРХ, в частности, такой ее элемент, как личность преступника, основным наиболее рациональным критерием их классификации

¹ © Чехович А. А., 2025.

будет уровень владения СКТ. По этому критерию можно выделить две группы преступников. К первой группе будут относиться преступники высокого уровня владения СКТ, обладающие навыками написания кодов программных продуктов, способные на сокрытие своего сетевого присутствия, путем уничтожения всевозможных следов противоправной деятельности, другими словами, способные оказывать активное противодействие раскрытию совершенного преступления. Такого рода преступники действуют либо в одиночку, когда преследуют определенные личные цели, либо группой, когда их цель НДКИ большая материальная выгода.

Вторую группу составят преступники, обладающие минимальными знаниями уровня базового пользователя СКТ, способные использовать приемы социальной инженерии, либо получить в теневом сегменте сети Интернет «Даркнет» необходимые сведения, такие как идентификационные данные и пароли владельцев банковских карт, специально разработанное программное обеспечение для подбора идентификационных данных потенциальной жертвы, преследующие цель получить незначительные материальные блага от НДКИ. Такие преступники редко обладают навыками противодействия раскрытию совершенного преступления, оставляют цифровые следы своей противоправной деятельности, не прикладывая особых усилий для их сокрытия. Как правило, реализуют свой преступный умысел исключительно ради получения материальных благ, мести и др.

Таким образом, личность преступника как элемент ОРХ, имеет определенное значение для предупреждения и раскрытия НДКИ. Личность преступника влияет на способ совершения НДКИ, орудия совершения НДКИ. Эти элементы ОРХ НДКИ находятся в непосредственной причинно-следственной взаимосвязи. Личность преступника в ОРХ НДКИ выступает системообразующим элементом, определяющим тактику оперативно-розыскных мероприятий. Дифференциация преступников на группы по уровню владения СКТ позволяет оптимизировать ресурсы правоохранительных органов и повысить эффективность раскрытия преступлений. Дальнейшая разработка ОРХ требует интеграции междисциплинарных подходов, включая IT-экспертизу, криминальную психологию и анализ больших данных.

Список литературы

1. Гребельский Д. В. О соотношении криминалистических и оперативно-розыскных характеристик преступлений // Криминалистическая характеристика преступлений : сб. науч. тр. / Всесоюзный институт по изучению причин и разработке мер предупреждения преступности ; редкол.: В. В. Клочков (отв. ред.), Л. Н. Викторова, В. А. Образцова, А. А. Эйсмана. М., 1984. С. 70–73.

2. Абрамов А. М. К вопросу о содержании оперативно-розыскной характеристики вида преступлений / А. М. Абрамов, И. А. Климов // Актуальные вопросы борьбы с преступностью и проблемы их преподавания : сб. науч. тр. / Моск. юрид. ин-т МВД России. М., 1996. С. 83–84.

3. Басецкий И. И. Квартирные кражи: теория и практика борьбы : монография / И. И. Басецкий, В. Ч. Родевич ; под ред. И. И. Басецкого. Минск : Академия МВД Республики Беларусь, 1999.

4. Козлов В. Е. Теоретико-прикладные аспекты первоначального этапа расследования компьютерных преступлений : дис. ... канд. юрид. наук : 12.00.09. Минск, 2000.

5. Лепехин А. Н. Криминалистическое обеспечение расследования преступлений против информационной безопасности : дис. ... канд. юрид. наук : 12.00.09. Минск, 2007.

Шаевич А. А.¹,
*старший преподаватель кафедры
информационных технологий
Восточно-Сибирского института МВД России,
кандидат юридических наук, доцент*

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ И ЭТИЧЕСКИЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТЕЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

За несколько последних лет нейросети уже внесли и продолжают вносить революционные изменения в различных сферах жизни, включая образование, медицину, транспорт и т. д. Не осталась в стороне и правоохранительная деятельность. Однако его внедрение сопровождается серьезными правовыми и этическими вызовами, которые требуют внимания со стороны законодателей, разработчиков и общества в целом. При этом, по нашему мнению, вопросы организации технических, программных и процессных аспектов использования искусственного интеллекта (далее – ИИ) в борьбе с преступностью неотрывно связаны с этической стороной вопроса, а то, что все это подлежит тщательной правовой регламентации, представляется очевидным. Таким образом, этику, организацию и правовое обеспечение следует рассматривать комплексно.

Как и любое другое достижение науки и техники, с момента появления ИИ, способного эффективно решать задачи по обработке больших массивов данных, генерировать фотоизображения, видео или аудио, он стал использоваться как для совершения преступлений, так и для борьбы с ними. Примеров успешного использования этих технологий для совершения преступлений уже очень много. В данной публикации не будем останавливаться на них подробно, отметим лишь, что, к сожалению, в деле совершения преступлений нейросети применяются намного чаще и эффективнее, чем в деле борьбы с ними. С другой стороны, уже есть примеры, когда использование нейростей в процессе судопроизводства повлекло к негативным последствиям. Так, например, широкую огласку получило расследование по делу судьи в Бразилии, который использовал искусственный интеллект и принял решения на основании ложной судебной практики. В частности, ChatGPT ссылался на резолюции Верховного суда, которых просто не существует. Чат-бот сформулировал для судьи решение, в котором эти резолюции он использовал в качестве основы для решения, вынесенного в постановлении [1–2].

«Казус Падильи» представляет собой первый зафиксированный прецедент применения системы ChatGPT для подготовки судебного акта. Однако использование технологий искусственного интеллекта (ИИ) в рамках судебных и досудебных процедур уже давно перестало быть инновацией в глобальном контексте. Многочисленные государства активно интегрируют ИИ-технологии в досудеб-

¹ © Шаевич А. А., 2025.

ные и судебные процессы, охватывающие производство по гражданским, уголовным и административным делам. Поэтому, закономерно, что тема обеспечения законности и этичности применения систем искусственного интеллекта в борьбе с преступностью привлекает внимание как отечественных, так и зарубежных исследователей.

Проведенный анализ публикаций затрагивающих эту тему, показал, что отечественные авторы в рамках диссертационных исследований [3, с. 163–211], публикаций в периодических научных изданиях [4, 5], в своих заключениях близки к выводам, к которым приходят зарубежные авторы [6, 7], что говорит об общих проблемах, несмотря на отличия в законодательстве и некоторых специфических отличиях в подходах к расследованию преступлений. Обобщенно, проблемы использования ИИ в расследовании преступлений, можно выразить следующим образом. К этическим проблемам относятся:

1. Проблема прозрачности и объяснимости решений ИИ.

Одной из ключевых этических проблем использования ИИ в расследовании преступлений является непрозрачность алгоритмов, на основе которых принимаются решения. Современные системы ИИ, особенно те, что основаны на машинном обучении, часто работают как «черные ящики»: даже разработчики не всегда могут точно объяснить, как именно система пришла к тому или иному выводу. Это создает серьезные проблемы для правоприменителей, которые должны быть уверены в обоснованности и законности своих действий. Например, если ИИ используется для прогнозирования вероятности совершения преступления конкретным лицом, важно понимать, на каких данных и алгоритмах основан этот прогноз. Недостаток прозрачности может привести к ошибкам, дискриминации и нарушению прав граждан. В случае, если решение ИИ становится основанием для задержания или избрания меры пресечения, это может привести к серьезным последствиям для личности, особенно если прогноз оказался ошибочным.

2. Дискриминация и предвзятость алгоритмов.

Еще одной серьезной этической проблемой является возможность дискриминации и предвзятости в алгоритмах ИИ. Системы ИИ обучаются на больших массивах данных, и если эти данные содержат предубеждения или исторически сложившиеся стереотипы, то ИИ может воспроизводить и усиливать эти предубеждения. Например, если в данных, на которых обучается система, преобладают случаи преступлений, совершенных представителями определенной социальной группы, ИИ может начать ассоциировать эту группу с повышенным риском преступности, что приведет к дискриминации. Примером такой проблемы является использование системы COMPAS в США, которая применялась для оценки риска рецидива у обвиняемых. Исследования показали, что система была склонна к расовой дискриминации, чаще предсказывая высокий риск рецидива для афроамериканцев по сравнению с белыми обвиняемыми. Это подчеркивает необходимость тщательной проверки данных и алгоритмов, используемых в системах ИИ, чтобы избежать дискриминации и нарушения прав граждан.

3. Нарушение права на частную жизнь.

Использование ИИ в расследовании преступлений часто связано с обработкой больших объемов персональных данных, включая биометрическую информацию, такую как изображения лиц, голосовые данные и даже данные о поведении. Это создает угрозу нарушения права на частную жизнь, особенно если данные собираются и обрабатываются без должного согласия граждан. Например, технологии распознавания лиц, которые активно используются для выявления подозреваемых, могут быть применены для массового наблюдения за гражданами, что противоречит принципам уважения частной жизни. В Европейском Союзе уже введены ограничения на использование таких технологий в публичных местах, чтобы защитить права граждан. В России также необходимо разработать четкие правила использования биометрических данных, чтобы предотвратить злоупотребления и обеспечить защиту прав личности.

4. Ответственность за решения, принятые ИИ.

Еще одной этической проблемой является вопрос ответственности за решения, принятые с использованием ИИ. Если система ИИ ошибается, кто несет за это ответственность: разработчик системы, правоохранительные органы или судья, который принял решение на основе рекомендаций ИИ? Этот вопрос особенно актуален в уголовном судопроизводстве, где ошибки могут привести к серьезным последствиям для личности, включая необоснованное лишение свободы. В настоящее время законодательство многих стран, включая Россию, не предусматривает четких правил ответственности за решения, принятые с использованием ИИ. Это создает правовой вакуум, который может быть использован для уклонения от ответственности. Необходимо разработать механизмы, которые позволят четко определить, кто и в какой степени несет ответственность за решения, принятые с использованием ИИ.

К организационным проблемы использования ИИ в расследовании преступлений относятся:

1. Неравномерный уровень технического оснащения.

Одной из основных организационных проблем является неравномерный уровень технического оснащения правоохранительных органов. В то время как некоторые регионы и ведомства активно внедряют современные технологии ИИ, другие продолжают работать с устаревшими системами и методами. Это создает дисбаланс в эффективности расследований и может привести к неравенству в доступе к правосудию.

2. Недостаток квалификации сотрудников.

Еще одной организационной проблемой является недостаток квалификации сотрудников правоохранительных органов в области ИТ-технологий. Многие сотрудники, особенно старшего поколения, не имеют достаточных знаний и навыков для работы с современными системами ИИ. Это может привести к ошибкам в использовании технологий и снижению эффективности их применения.

3. Недостаток нормативного регулирования.

Одной из ключевых организационных проблем является недостаток нормативного регулирования использования ИИ в уголовном судопроизводстве. В настоящее время отсутствуют четкие правила и стандарты, регулирующие

применение технологий ИИ в расследовании преступлений. Это создает правовой вакуум, который может быть использован для злоупотреблений и нарушений прав граждан.

В заключение можно сказать, что использование искусственного интеллекта в расследовании преступлений, безусловно, открывает новые возможности для повышения эффективности работы правоохранительных органов. Однако внедрение этих технологий сопряжено с рядом этических и организационных проблем, которые требуют тщательного анализа и разработки механизмов их решения. Для успешного внедрения ИИ в уголовное судопроизводство необходимо обеспечить прозрачность и объяснимость решений, минимизировать риски дискриминации, защитить право на частную жизнь, а также разработать четкие правила ответственности за решения, принятые с использованием ИИ. Кроме того, важно решить организационные проблемы, связанные с техническим оснащением, которое может существенно отличаться в крупных городах и небольших удаленных населенных пунктах. Кроме того, с учетом кадровой проблемы в системе МВД России в настоящее время вопрос квалификации сотрудников, представляет собой отдельную проблему. Только при условии комплексного подхода к решению этих проблем можно обеспечить эффективное использование ИИ в расследовании преступлений, которое не будет приводить к незаконным ограничениям конституционных прав граждан.

Список литературы

1. Бот судья: чем грозит применение искусственного интеллекта в судах // URL: <https://www.forbes.ru/mneniya/484998-bot-sud-a-cem-grozit-primenenie-iskusstvennogo-intellekta-v-sudah>.
2. Под следствие попал судья, приговоры которому писал ChatGPT // URL: https://www.cnews.ru/news/top/2023-11-14_v_brazilii_sudya_popal_pod.
3. Чурикова А. Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование : дис. ... д-ра юрид. наук. Саратов, 2024.
4. Воробьева И. Б. Этические аспекты использования систем искусственного интеллекта при расследовании преступлений // Вестник Саратовской государственной юридической академии. 2022. № 4 (147). С. 162–172.
5. Лиманский Н. Н. Внедрение искусственного интеллекта: анализ правовых проблем и международный опыт // Океанский менеджмент. 2024. № 3 (27). С. 59–62.
6. The Ethical Implications of AI in Forensic Science // Forensic Science Academy. URL: <https://forensicscienceacademy.org/blog/f/the-ethical-implications-of-ai-in-forensic-science>.
7. Hunter Dan, Mirko Bagaric, Nigel Stobbs. A framework for the efficient and ethical use of artificial intelligence in the Criminal Justice System // Florida State University Law Review , vol. 47, 2020, pp. 749–800.

Шайдаев М. Ш.¹,
*ведущий научный сотрудник
Центра сопровождения научно-исследовательских
и опытно-конструкторских работ
в области информационных технологий
Научно-исследовательского института
специальной техники ФКУ НПО
«СТиС» МВД России,
кандидат юридических наук*

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ, ПОЛОВОЙ СВОБОДЫ И НРАВСТВЕННОСТИ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие и внедрение информационных технологий, с одной стороны, приносит существенные преимущества в обеспечении жизнедеятельности человека. С другой – предоставляет криминалитету огромное количество возможностей в приискании новых способов совершения преступлений.

Уровень противоправных деяний с использованием информационно-коммуникационных технологий превысил уже все допустимые пределы, а разнообразность их растет с каждым днем.

С развитием интернет-технологий и сотовой связи одновременно с обеспечением коммуникации, находящимся в различных городах и странах абонентам, получения необходимой информации, оплаты услуг и покупок в онлайн-магазинах и т. д. была создана благоприятная среда для совершения противоправных деяний с их применением [1, с. 48].

Уголовный кодекс Российской Федерации содержит порядка 25 составов преступлений, предусматривающих квалифицирующий признак – совершение деяния с использованием средств массовой информации или информационно-телекоммуникационных сетей (включая сеть Интернет). К ним относятся отдельные виды преступлений против жизни и здоровья, семьи и несовершеннолетних, различные виды мошенничества, в сфере незаконного оборота наркотических, лекарственных и аналогичных им средств, против общественной безопасности и общественного порядка, основ конституционного строя и безопасности государства, мира и безопасности человечества.

Одним из наиболее опасных видов криминальной активности, отличающихся в последние годы негативной динамикой роста, признаются преступления против половой свободы, половой неприкосновенности и нравственности. Специалистами отмечается, что с развитием информационных технологий ускоряется тенденция перемещения указанных преступлений в информационную среду. Сексуальное насилие и эксплуатация посредством использования информационно-коммуникационных технологий приобретают глобальный характер [2, с. 183].

¹ © Шайдаев М. Ш., 2025.

Развитию такой ситуации, на наш взгляд, способствовало как минимум два создавших благодатную почву для совершения указанных противоправных деяний обстоятельства. Во-первых, это изначальная бесконтрольность печатных средств массовой информации, а в последующем телекоммуникационных систем и сети Интернета, площадки которых стали использоваться для открытого и повального размещения продукции эротического и порнографического характера. Во-вторых, беспрепятственная и простая регистрация в социальных сетях неограниченного количества страниц для размещения указанной продукции [1, с. 49].

По данным различных европейских источников в Евросоюзе только в отношении детей количество сведений о контенте, содержащем сексуальное насилие над ними, с 2010 по 2019 г. выросло с 23000 до 750000, т. е. почти в 33 раза. За 2020 г. на 28% по сравнению с 2019 г. увеличилось количество сообщений о сексуальной эксплуатации детей. В некоторых странах Европы такая негативная динамика возросла в разы: в Польше – в 5 раз, в Испании в 2 раза, в других странах чуть меньше, но это также доказывает катастрофичность проблемы. Буквально за два месяца (май–июнь) 2021 г. почти в два раза с 8000 до 14000 увеличилось количество обращений от поставщиков электронных услуг об обнаружении ими материалов о сексуальном насилии [3, с. 78; 4, с. 613–614]. Аналогичная ситуация, хоть и в не таких масштабах, складывалась и в нашей стране.

По статистическим данным за период с 2018 по 2023 гг. посягательств на общественную нравственность с использованием информационно-телекоммуникационных и цифровых технологий зарегистрировано более 13 тыс. [5, с. 222]. За этот же период преступлений против половой свободы и половой неприкосновенности, совершенных бесконтактно с использованием информационно-коммуникационных технологий, зарегистрировано около 18 тыс. [5, с. 87].

Особую тревогу вызывает рост преступности с использованием цифровых технологий в отношении несовершеннолетних. Увлеченные виртуальным миром, подолгу проводящие время в социальных сетях и мессенджерах подростки в открытом доступе могут наблюдать видеоролики, содержащие сцены сексуального насилия и домогательства, оказаться под давлением распространяющегося культа жестокости и насилия, сексуальной распущенности. Данный контент оказывает деструктивное влияние не только на психическое и психологические развитие несовершеннолетних, но и на их поведение.

Уязвимость детей в цифровой среде, обусловленная их повышенной восприимчивостью негативных действий, открывает возможность преступникам или лицам, страдающим сексуальными расстройствами, такими как педофилия, приобретать свою целевую аудиторию [1, с. 50; 6, с. 91]. А, обладая информационной грамотностью, профессиональными знаниями цифровых технологий, соответствующими навыками и умениями, указанный асоциальный контингент оказывает деструктивное воздействие на детей и подростков с целью их вовлечения в совершение противоправных деяний.

На сегодняшний день злоумышленники чаще всего используют для бесконтактного развращения подростков такие каналы передачи электронной информации как: социальные сети, электронная почта, мобильные приложения типа

WhatsApp, Instagram, Facebook¹, Twitter (X), сайты знакомств, форумы и чаты. Специалистами признается, что практически каждый третий несовершеннолетний, не достигший возраста шестнадцати лет, получал сообщение сексуального содержания от незнакомого лица [7, с. 148; 8, с. 123].

Исходя из имеющейся статистики, за период 2018–2023 гг. зарегистрировано 2126 преступлений против нравственности, совершенных в отношении несовершеннолетних, с использованием информационно-телекоммуникационных технологий. Преступлений против половой свободы и половой неприкосновенности в отношении несовершеннолетних с использованием информационно-телекоммуникационных технологий за период 2021–2023 годы зарегистрировано 19260 преступлений (в 2021 г. – 5450, в 2022 г. – 6141, в 2023 г. – 7669). За это же время потерпевшими по указанным преступлениям признано 2822 несовершеннолетних [5, с. 222–225].

Наблюдаемый ежегодный рост их количества обусловлен как широким распространением высоких технологий среди населения, в том числе несовершеннолетних, так и быстрым освоением их возможностей для совершения противоправных деяний, к которым можно отнести:

- возможность обеспечения анонимности своих действий по отношению к подвергаемой обработке личности;
- возможность сокрытия цифровых следов преступлений;
- возможность обеспечения единовременного коммуницирования с большим количеством несовершеннолетних;
- отсутствие границ в поиске очередного объекта для воздействия;
- латентный характер совершаемых преступных деяний [7, с. 149].
- Специалистами рассматривается три основных способа совершения половых преступлений с использованием ИТТ:
 - осуществление в социальных сетях или мессенджерах шантажа в виде угрозы распространить компрометирующие сведения о лице, вынуждая его совершить действия сексуального характера;
 - передача в социальных сетях или мессенджерах лицу, заведомо не достигшему шестнадцатилетнего возраста, порнографических фотоизображений и (или) видеозаписей (онлайн-груминг);
 - проведение с помощью информационно-коммуникационных сетей и мессенджеров либо мобильной связи бесед сексуального содержания с лицами, не достигшими шестнадцатилетнего возраста [9, с. 34].

Кроме того, преступники осваивают и быстро внедряют в свою преступную деятельность новые информационные технологии, в том числе технологии искусственного интеллекта. Создавая на их основе совершенно новые бизнес-модели, стремятся активно их применять при совершении преступлений, особенно в отношении несовершеннолетних.

¹ WhatsApp, Instagram, Facebook принадлежат компании Meta, признанной экстремистской и запрещенной на территории Российской Федерации. *Здесь и далее по тексту.*

Учитывая новые формы и способы совершения противоправных деяний против половой свободы, половой неприкосновенности личности и нравственности с использованием цифровых технологий, разрабатываемые меры противодействия должны быть направлены на обеспечение надежной защиты пользователей информационно-коммуникационных сетей, и в первую очередь подростков и малолетних, от деструктивного воздействия. Для этих целей государством создается комплекс нормативно-правовых, организационных, воспитательных, образовательных, методологических, информационно-технологических и иных механизмов противодействия.

Кроме этого, крайне важно опережающими темпами вооружить правоохранительные органы новыми технологическими и информационными инновациями, благодаря которым откроется доступ к большому числу инструментов, обеспечивающих эффективное противодействие этим новым криминальным угрозам.

Среди цифровых технологий, обеспечивающих предотвращение негативного влияния сети Интернет на несовершеннолетнего, ограничивающих посещение подозрительных сайтов, а также длительное пребывание в интернет-пространстве, в современной России стали популярны такие технологии, как программа «родительский контроль», «детский режим».

Подобные программы, получившие название «кибер-нянь», но с более расширенным функционалом упреждающего характера активно уже применяются в Америке и странах Европы. Предназначены они для выявления деструктивного, негативного и запрещенного контента, а также нейтрализации и предупреждения онлайн-рисков, связанных непосредственно с вовлечением несовершеннолетних в противоправную деятельность и совершением в отношении них преступлений. Мониторя в автоматическом режиме используемые несовершеннолетними интернет-ресурсы, социальные сети и мессенджеры, указанные программы способны выявлять лиц, использующих социальные сети для совершения развратных действий с несовершеннолетними и распространения материалов порнографического характера, одновременно перекрывая доступ детям к пользованию сайтами аморального и жестокого характера после их обнаружения [7, с. 149–150].

К иным механизмам защиты детей и подростков от сексуального насилия в сети Интернет, осуществляющие досудебное блокирование сайтов с детской порнографией, относятся специализированные центры, предназначенные для обеспечения безопасного пользования всемирной сетью без риска стать жертвой преступления. В совершенствовании мер, позволяющих повысить уровень информационно-цифровой безопасности несовершеннолетних, в настоящее время существенное значение придается внедрению современных технологий искусственного интеллекта. Международный опыт свидетельствует, что в мире уже созданы и используются нейросетевые алгоритмы анализа информационно-цифрового окружения детей и подростков и распознавания опасного для детей контента. Использование в них современных нейросетей при мониторинге сети Интернет позволяет на основе оперативного анализа больших объемов данных, многочисленных видеопотоков, эффективно идентифицировать преступников, выявлять и блокировать запрещенный контент и предотвращать тяжкие преступления.

Подобные аналитические продукты, работающие на основе технологий искусственного интеллекта, уже нашли свое место на рынке информационных технологий:

Платформа SemanticForce (Семантик Форс). Способна на основе мониторинга социальных сетей, отзывов, новостей, мессенджеров, в том числе путем отслеживания разговоров, распознавать намерения, выявлять тенденции, закономерности и аномалии. Платформа может формировать различные базы данных: онлайн-видео, мессенджеров, онлайн-СМИ, блогов, социальных сетей. Основными ее функциями являются анализ источников, оценка воздействия, контент-анализ, интеллектуальный анализ информации.

Аналитический онлайн-сервис Data Plexus (Дата Плексус), позволяющий в единой системе решать задачи сбора больших объемов данных, медиа-аналитики, извлечения и анализа информации из разнородных открытых и закрытых источников данных, выявления значимых фактов и событий с последующим оповещением.

Онлайн-сервис Meltwater (Мелтвотер), являющийся одним из лидерских продуктов на американском рынке в области онлайн-мониторинга СМИ и медиа-аналитики, предназначена для просеивания новостей, публикаций в социальных сетях и других типов сообщений. Основанная на искусственном интеллекте технология мониторинга СМИ в сочетании с глобальной сетью обеспечивает доступ к контенту на местном, национальном и глобальном уровнях.

К числу ведущих американских программных продуктов для анализа социальных данных относится также Интернет-сервис Talkwalker (Толкволкер, Говорун), который предназначен для работы в социальных сетях и аналитики социальных медиа. К его ключевым функциям относятся контент-анализ, интеллектуальная обработка медиа-данных, анализ настроений и тональности сообщений на основе искусственного интеллекта, распознавание видео.

Среди отечественных аналогов следует упомянуть систему аналитики и мониторинга социальных медиа «Медialogия SM», которая собирает и анализирует данные из 2,5 млрд источников соцмедиа (соцсети, видео-платформы, блоги-форумы, мессенджеры и СМИ), обрабатывает тексты, картинки, локации, видео и истории, и по итогам анализа формирует подробный отчет.

Система мониторинга СКАН-Интерфакс отслеживает и анализирует сообщения в СМИ соцсетях, соцмедиа, форумах и блогах в режиме реального времени, формируя визуальные аналитические отчеты по любым запросам. Система оперативного и ретроспективного мониторинга Крибрум.Про обеспечивает количественный и качественный анализ СМИ, социальных медиа и телеграм-каналов. Его функциональные возможности включают мониторинг социальных медиа, сбор, хранение и обработка сообщений, автоматическое определение эмоционального отношения автора к объекту высказывания, выявление исходных источников сообщений. Использование указанных и им подобных аналитических продуктов на основе нейросетей и искусственного интеллекта позволит существенно улучшить работу правоохранительных органов, обеспечив более эффективную борьбу с указанным видом преступности.

Таким образом, признавая, что преступления сексуального характера против несовершеннолетних с использованием интернет-ресурсов представляют серьезную опасность нормальному психологическому и нравственному развитию несовершеннолетних, необходимо обеспечить максимальную защиту данных лиц от подобных посягательств. Разработка и внедрение на основе цифровых технологий новейших методов предотвращения развращения несовершеннолетних через всемирную сеть, выявления, пресечения и раскрытия ненасильственных половых преступлений позволит защитить подрастающее поколение от преждевременной сексуализации и ее негативных последствий, а значит, будет способствовать нормальному и гармоничному развитию подрастающего поколения страны.

Список литературы

1. Скобина Е. А. Преступления против половой свободы и половой неприкосновенности в отношении несовершеннолетних с использованием интернет-пространства // Юридические науки: проблемы и перспективы : материалы VIII Междунар. науч. конф. Казань : Молодой ученый, 2019. С. 48–53.
2. Михайлова Е. В. Криминологическая характеристика преступлений против половой свободы и половой неприкосновенности несовершеннолетних, совершаемых с использованием информационно-телекоммуникационных технологий // Вестник Московского университета МВД России. 2022. № 1. С. 182–188.
3. Рыжков В. Б. Взаимодействие государств-участников Европейского Союза в борьбе с сексуальной эксплуатацией детей и детской порнографией // Вестник экономической безопасности. 2019. № 2. С. 139–144.
4. Шуняева В. А. Защита половой неприкосновенности несовершеннолетних в сети Интернет // Актуальные проблемы государства и права. 2022. Т. 6. № 4. С. 611–617.
5. Пинкевич Т. В. и др. Преступления против нравственности, половой свободы и половой неприкосновенности личности: уголовно-правовой, криминологический и психологический аспекты : аналитический обзор с предложениями и видеоколлекцией. М. : Академия управления МВД России, 2024.
6. Семенцова И. А. Актуальные вопросы предупреждения преступлений, совершаемых лицами с расстройствами сексуального предпочтения (педофилией) посредством сети Интернет / И. А. Семенцова, А. И. Фоменко // Теория и практика общественного развития. 2015. № 10. С. 90–93.
7. Скворцова О. Д., Макаренко Д. Д. Развратные действия с использованием сети Интернет // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2021. Т. 7 (73). № 1. С. 146–153.
8. Соловьев В. С. Использование социального сегмента сети Интернет для совершения посягательств на половую неприкосновенность несовершеннолетних // Вестник Московского университета МВД России. 2017. № 3.
9. Примаков А. Н. Об информационно-телекоммуникационных способах совершения преступлений против половой неприкосновенности и половой свободы // Вестник Могилевского института МВД. 2022. № 2 (6). С. 32–36.

Шавловский А. Б.¹,
*преподаватель кафедры судебно-экспертной
и оперативно-розыскной деятельности
Московской академии Следственного комитета
Российской Федерации имени А.Я. Сухарева*

ПРАКТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННО- АНАЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ ОТКРЫТЫХ ИСТОЧНИКОВ СЕТИ ИНТЕРНЕТ

В настоящее время наблюдается устойчивая тенденция роста преступлений, совершаемых с использованием информационно-коммуникационных технологий. Так, по данным МВД России, в 2024 г, было зарегистрировано на 13,1 % больше киберпреступлений по сравнению с 2023 г. [1]. Указанная тенденция обусловлена сложностью расследования киберпреступлений, поскольку современные киберпреступники умело используют и совершенствуют достижения науки и техники в противоправной деятельности, осваивают узконаправленные профессиональные компетенции, среди которых можно выделить следующие:

- использование технологий искусственного интеллекта для создания, обработки или изменения видеоизображений, имитации голоса и речи человека в звукозаписях;
- использование цифровой валюты (криптовалюты) для легализации (отмывания) денежных средств;
- использование сервисов обмена электронными сообщениями (т. н. «мессенджеры»), оснащенных технологиями повышенной анонимности.

Вопросы использования сети Интернет в раскрытии и расследовании преступлений являются предметом изучения со стороны различных ученых. Так, А. Т. Анешева, К. С. Сидорова выделяют одно из направлений использования сети Интернет в расследовании преступлений: «оптимизация процесса организации расследования и раскрытия преступлений» [2].

Среди других актуальных направлений использования сети Интернет в расследовании преступлений можно выделить: поиск и исследование информации, содержащейся в открытых источниках сети Интернет. Как подчеркивает О. А. Дворянкин, «с развитием интернета фокус внимания аналитиков сместился в киберпространство как один из главных источников информации» [3].

В связи с изложенным в условиях роста количества совершаемых киберпреступлений вопрос исследования информации в открытых источниках сети Интернет представляет научно-методический интерес и практическое значение в целях раскрытия, расследования и предупреждения преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Методы и средства поиска информации в открытых источниках сети Интернет в своей совокупности именуется как технология OSINT (с англ. яз. – «Open

¹ © Шавловский А. Б., 2025.

source intelligence»). А. А. Бессонов характеризует данную технологию, как совокупность методов, именуемых как «поиск и анализ информации из открытых источников» [4].

В настоящее время технология OSINT применяется в практической деятельности правоохранительных органов Российской Федерации. В Следственном комитете Российской Федерации ее используют следователи, специалисты криминалистических подразделений, в том числе Главного управления криминалистики (Криминалистического центра), а также эксперты Судебно-экспертного центра Следственного комитета Российской Федерации. В подразделениях Судебно-экспертного центра Следственного комитета Российской Федерации технология OSINT применяется при проведении следственных осмотров ресурсов сети Интернет, а также при проведении информационно-аналитических исследований открытых источников сети Интернет.

Назначение информационно-аналитических исследований в Судебно-экспертном центре Следственного комитета Российской Федерации регулируется приказом Судебно-экспертного центра Следственного комитета Российской Федерации от 12.05.2022 № 22-сэц [5], в котором в качестве основания для производства исследования определено постановление (отношение) о назначении исследования, вынесенное лицом, уполномоченным проводить расследование. В указанном отношении должна содержаться информация об инициаторе, его контактных данных, краткие обстоятельства уголовного дела (фабула) или материалов проверки, а также сформулированный запрос на проведение информационно-аналитического исследования в открытых источниках сети Интернет с указанием установочных (поисковых) данных.

В качестве установочных данных для выполнения информационно-аналитических исследований инициатором предоставляются идентификационные и другие сведения, позволяющие выделить ключевую информацию о предмете поиска из массива цифровых данных. В качестве таких данных могут быть предоставлены: абонентский номер, фамилия, имя и отчество, дата рождения лица, псевдоним, адрес учетной записи в социальной сети или мессенджере, иные сведения о физических, юридических лицах, о движимом или недвижимом имуществе.

Исходя из практики выполнения информационно-аналитических исследований, в открытых источниках сети Интернет возможно обнаружить следующие сведения о деятельности пользователей:

- данные, ассоциированные с работой пользователей в интернет-сервисах (например: по доставке еды и оказанию услуг): абонентские номера, адреса электронных почт, места жительства, опубликованные отзывы на оказанные услуги;
- данные, содержащиеся в социальных сетях и сервисах обмена электронными сообщениями: идентификаторы страниц пользователей и сообществ, имена и псевдонимы пользователей, сведения о возрасте, месте жительства, образовании, месте работы, интересах, подписках на новостные каналы и сообщества, размещенные аудиозаписи, видеозаписи, фотоизображения, публикации, комментарии, реакции (лайки), хештеги, координаты местоположений, пользователи в категории «друзья»;

- данные, ассоциированные с деятельностью пользователей на информационных ресурсах (веб-сайтах): имена и псевдонимы пользователей, размещенные объявления, отзывы, записи, сообщения, аудиозаписи, видеозаписи, фотоизображения;
- данные, содержащиеся в официальных базах и документах, размещенных на информационных ресурсах: базы судебных решений, базы решений административных органов, официальные документы и решения федеральных, региональных и муниципальных органов, государственные реестры (например: единый государственный реестр индивидуальных предпринимателей);
- данные, ассоциированные с криптовалютной деятельностью: сведения об адресах криптовалютных кошельков, выполненных операциях и транзакциях.

Таким образом, открытые источники сети Интернет представляют практический интерес для правоохранительных органов, так как расширяют их возможности в решении поисковых задач, установлении обстоятельств уголовных дел. В условиях необходимости повышения эффективности противодействия преступлениям в сфере информационно-коммуникационных технологий вопросы использования в правоохранительной деятельности методов и средств поиска и исследования информации в сети Интернет, подлежат анализу с целью выработки соответствующих методических и практических рекомендаций.

Список литературы

1. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2024 г. // Официальный сайт МВД России. URL: <https://мвд.рф/reports/item/60248328/>.
2. Анешева А. Т., Сидорова К. С. К вопросу о возможностях использования информационно-телекоммуникационной сети Интернет в организации раскрытия и расследования преступлений // Пенитенциарная система и общество: опыт взаимодействия : сборник материалов V Международной научно-практической конференции. Пермь : Пермский институт Федеральной службы исполнения наказаний, 2018. С. 206–208.
3. Дворянкин О. А. Osint, pentest и нетсталкинг - информационные технологии Интернета // Национальная Ассоциация Ученых. – 2022. – № 84-2. – С. 6–13.
4. Бессонов А. А. Современные возможности технологии поиска информации из открытых источников в расследовании преступлений // Цифровые технологии современной криминалистики, использование специальных знаний : материалы конференции, проведенной в рамках Международного форума «Интерполитех: цифровая трансформация безопасности государства». М. : Московская академия следственного комитета, 2023. С. 48–58.
5. Приказ федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации» от 12.05.2022 № 22-сэц «О некоторых вопросах организации производства судебных экспертиз (исследований) в федеральном государственном казенном учреждении “Судебно-экспертный центр Следственного комитета Российской Федерации”» // НПП «Гарант-сервис».

РАЗДЕЛ III. ВИДЫ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С РАСПРОСТРАНЕНИЕМ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

Аксенов А. В.¹,

*курсант Института-факультета подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Токолов А. В.,

*доцент кафедры противодействия
преступлениям в сфере информационно-
телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук*

МЕТОД СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, КАК СРЕДСТВО ДОСТИЖЕНИЯ ЦЕЛЕЙ КИБЕРПРЕСТУПЛЕНИЙ

До появления сети Интернет многие сферы жизни общества были крайне неудобны в своей реализации. К основным таким сферам стоит отнести: обмен данными и информацией, получение услуг, различного рода хранилища информации, распространение информации, а также документооборот.

Стоит более детально рассмотреть обмен данными и информацией. Данная отрасль представляет собой процесс получения данных от субъекта к субъекту. В данном случае субъектами таких отношений выступают отправитель и получатель. До изобретения сети Интернет такой обмен происходил самыми различными способами. Например, в 1800-х гг. люди отправляли письма голубиной почтой, такая почта получила распространение не только за рубежом, но и в России. Так же люди писали письма перьями на бумаге и направляли их почтой, человек работавший почтальоном самостоятельно пересылали письма адресатам. Разумеется, в рассмотренных выше способах обмен происходил не столь быстро, как в нынешнее время, когда, например, отправляется сообщение в социальных сетях. Затрагивая тему социальных сетей, которые напрямую связаны с сетью интернет, необходимо сказать, что благодаря интернету общение между людьми стало гораздо проще. Благодаря информационно-телекоммуникационной сети людям не нужно покидать свое жилище для того, чтобы передать сообщение кому-нибудь или получить какую-либо услугу.

¹ © Аксенов А. В., 2025.

Несмотря на удобство технологий, которые появились сравнительно недавно, как и любые сферы жизни, они имеют определенные недостатки. К основному из них следует отнести возможность получать чужие денежные средства путем обмана и злоупотребления доверием, т. е. используя мошенничество. Чаще всего такие преступления совершаются с использованием методов социальной инженерии, в данной связи необходимо рассмотреть это понятие. Социальная инженерия - способ завладения чужими конфиденциальными данными, путем использования психологических способов убеждения и расположения жертвы к себе. Совершение киберпреступлений путем использования психологического влияния на человека стоит рассматривать, как один из самых сложных по структуре расследования киберпреступлений. Указанное утверждение рождается исходя из статистики, касаемой расследования киберпреступлений. Таким образом, количество киберпреступлений в 2024 г. возросло на 24,4 %, а мошенничество в данной сфере киберпреступлений занимает лидирующее место. Чаще всего такие преступления совершаются путем создания фальшивых ссылок на официальные сайты, создания сайтов двойников, звонков по видео или голосовой связи под видом сотрудников банков, ФСБ и полиции [1], взлома социальных сетей, а также применяются технологии дипфейков. Проблематика предотвращения таких преступлений заключается в том, что несмотря на многочисленные оповещения граждан о наличии мошенников в обществе, люди доверяют злоумышленникам, так как те используют различные способы воздействия и манипулирования. К таким инструментам манипуляции можно отнести такие как угрозы, давление, принятие или внушение роли спасателя. Также при расследовании данного вида преступлений сотрудники сталкиваются с рядом сложностей, таких как быстрое уничтожение вещественных доказательств злоумышленниками, обрывание связей с жертвой, обналичивание электронных денежных средств.

Для решения проблем расследования следует рассмотреть различные новые технологии, включая искусственный интеллект. Переводя денежные средства, жертва чаще всего использует мобильный телефон, на который установлен онлайн банк [2]. Возможно установить функцию, которая будет высылать уведомления на экран пользователей при переводе денежных средств, содержащие в себе памятку о мошеннических действиях, способах распознавания злоумышленников и дополнительную кнопку, подтверждающую перевод. Такая функция позволит задуматься о необходимости перевода средств, а также предотвратит неразумные переводы. Также возможно рассмотреть создание новых программ, блокирующих подозрительные ссылки и способных анализировать схожие ссылки и сайты, удаляя неофициальные и не сертифицированные. Такая технология позволит предотвратить подделку сайтов и ссылок.

Складывается впечатление, что сегодня перечень всех допустимых изобретений уже исчерпан. Однако преступность не стоит на месте, но появляются все новые и новые виды преступлений, совершаемых посредством информационно-телекоммуникационной сети Интернет. Необходимо отметить, что никакие аппаратные, программные и любые другие средства не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе

к вопросам безопасности компьютерных систем и их сетей, а также организации взаимодействия между субъектами выявления, раскрытия и расследования киберпреступлений на международном уровне.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// СПС «КонсультантПлюс».
2. Федоров М. Н. Преступления, совершаемые с помощью глобальной информационной сети Интернет.
3. Батулин Ю. М. Проблемы компьютерного права. М. : Юрид. лит., 1991.
4. Беспалова Е. В., Широков В. А. Киберпреступность: история уголовно-правового противодействия // Информационное право. Юрист. 2006. № 4 (7).
5. Дворецкий М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания : монография
6. Голубев В. А. Компьютерная преступность: состояние, угрозы и прогнозы // Компьютерная преступность и кибертерроризм. Сборник научных работ: вып. № 2. Запорожье : Центр исследования компьютерной преступности, 2004.
7. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. М. : Ай Пи Ар Медиа, 2025.
8. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. М. : Ай Пи Ар Медиа, 2025.
9. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. М. : Ай Пи Ар Медиа, 2025.
10. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. Саратов : М. : Профобразование : Ай Пи Ар Медиа, 2025.
11. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. М. : Московский университет МВД России имени В.Я. Кикотя, 2024. С. 35–37.

*Алексеева Г. П.¹,
курсант Института-факультета подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

*Научный руководитель:
Поликарпова Е. В.,
старший преподаватель кафедры
противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ХАКЕРСТВО КАК ВИД СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЯ XXI В.

В XXI в. преступления в информационной среде стали частым явлением. Многие ученые объясняют это развитием данной среды, развитием, так называемой, мировой паутины. Некоторые из ученых прогнозируют, скорое, развитие и повышение статистики совершения преступлений в информационной среде, другие же, напротив, не желают давать такие прогнозы и считают, что преступления в информационной сфере пойдут на спад.

Однако если обратиться к нынешней ситуации в сфере информационной преступности, можно сделать вывод, что подобные преступления становятся частым явлением и необходимо обратить пристальное внимание, как и на факт совершения данных преступлений, так и на их разновидность, статистику. Необходимо усовершенствовать меры противодействия данным видам преступлений.

В данной статье представлен один из видов совершения киберпреступлений, а именно – хакерство. Изначально, «хакерами» называли программистов, которые работали над исправлением ошибок в компьютерном обеспечении, однако, со временем и развитием мировой паутины, а также технологий, хакерами начали называть иных специалистов. С прогрессом в сфере технологий, развитием данной сферы, хакерами стали называть программистов, что с помощью своих знаний и умений, взламывают личные аккаунты людей на различных серверах и сервисах с целью похищения личной информации, которая впоследствии необходима для совершения различных преступлений, к примеру, мошенничеству, вымогательству на почве финансовой выгоды.

Данные случаи нередки, и зачастую подобные преступники связываются с жертвами, чья личная информация находится в руках преступников. Один из самых распространенных случаях, что стал будничностью XXI в. – телефонное мошенничество, связанное с похищенными данными. Осуществляя звонок

¹ © Алексеева Г. П., 2025.

какому-либо лицу мошенники, хакеры, во время разговора похищают информацию, выуживая их с помощью взлома сервиса, на платформе которого проходит звонок, мессенджеры. Говоря о хакерстве, также стоит отметить и другой вид похищения информации, который вскользь упоминался ранее, а именно скрытое похищение личных данных, например, реквизитов и код-паролей от банковских карт. Далее наступает иной этап – вымогательство или же тайное хищение денежных средств с банковской карты.

Стоит также отметить, что в истории имелись и более крупные случаи киберпреступности, а конкретнее – завладение секретной правительственной информации. Раскроем один из самых резонансных случаев в современной истории как пример.

Одним из самых известных хакеров считается Эдвард Джозеф Сноуден – американский бывший сотрудник ЦРУ [3], технический специалист и спецгент. Его называют гением многие технические специалисты, ведь его знания в данной сфере очень обширны и виртуозны. Активные действия данного специалиста начались в мае 2013 г., когда он связался с представителями различных сфер, по официальной информации это был журналист одного из изданий, кинорежиссер и кинопродюсер, с целью передачи важной информации. Передача информации и ведение разговоров было с помощью зашифрованных e-mail сообщений, не раскрывая своей личности. Дело касалось государственной программы США – PRISM [4]. Данная государственная программа Соединенных Штатов Америки, была принята Агентством Национальной безопасности и занималась негласным сбором информации, которая передавалась по сети, т. е. к ним относились телефонные звонки, личные сообщения и прочее. Квалифицировалась данная информация как совершенно секретная. Благодаря публикации в июне 2013 г., общественность узнала о подобной государственной программе, а также о характере собираемых данных. Был установлен и разглашен факт слежения в 60 странах правительствами 35 стран, были рассекреченные данные о слежке во многих мессенджерах, что благодаря этой государственной программе, правительство США, могло просматривать фотоматериалы и видеоматериалы, отслеживать пересылаемые пользователями данные. Данная публикация затрагивала не все секретные материалы, что относились к данной государственной программе, но раскрыла сам факт слежения, и характер данной информации, что был весьма весом, ведь также Сноуден раскрыл факт незаконного проникновения в компьютерные сети восточноазиатской волоконно-оптической сети Pacnet, а также китайских операторов мобильной связи для получения доступа к миллионам SMS, и многое иное. Данная публикация и раскрытие правды вызвало огромный резонанс в обществе, в то время как целью Сноудена было не навредить людям, а раскрыть часть происходящего за закрытыми дверями, то, что скрыто от людей, то, что те никогда не должны узнать. Было передано от 50 до 200 тыс. секретных документов, что подтвердил директор ранее упомянутого АНБ, генерал Кит Александер, комментируя, что все эти документы будут постепенно освещаться в СМИ.

После открытия правды данным бывшим агентом ЦРУ за ним началась слежка, из-за чего он скрывался от властей США в Гонконге и искал пристанище в иных странах, где ценится свобода слова. Тогда, пресс-секретарь Президента

Российской Федерации, Дмитрий Песков, упомянул о готовности России рассмотреть предложение о выдаче Эдварду Джоозефу Сноудену предоставления политического убежища в России, если таковая необходимость имеется и данное прошение поступит, что вскоре подтвердил Министр иностранных дел Российской Федерации Сергей Лавров. 23 июня 2013 г., после требования властей США к Гонконгу выдать им Сноудена, тот прибыл на территорию Российской Федерации в сопровождении представителя международной некоммерческой организации, публикующую секретную информацию. На данный момент Эдвард Джоозеф Сноуден проживает в России.

Данный пример можно охарактеризовать с нескольких сторон, однако, первостепенной для нашего исследования стоит отметить возможность получения секретной правительственной информацией. На примере данного хакера мы можем сделать вывод, что информационное пространство небезопасно и любую информацию возможно заполучить, имея определенные навыки. И, зачастую, данная информация идет во вред истинным владельцам. В Уголовном кодексе Российской Федерации также предусмотрена уголовная ответственность, связанная с ИТ-технологиями, а именно в главе 28, которая так и закрепляет «Преступления в сфере компьютерной информации». Касательно совершенных киберпреступлений на территории Российской Федерации, стоит отметить, что МВД России на своем информационном портале 20 апреля 2025 г. опубликовал краткую характеристику состояния преступности в Российской Федерации за январь–март 2025 г. Относительно интересующей нас сферы, МВД России сообщает, что: «По-прежнему более трети преступлений совершается с использованием информационно-телекоммуникационных технологий. Таких деяний зарегистрировано на 3 % больше, чем в январе-марте прошлого года.»

Исходя из вышесказанной информации, стоит отметить наличие роста подобных преступлений, несмотря на активное противодействие подобному виду совершения преступлений. Зачастую, жертвами киберпреступлений становятся люди в возрасте 60–75 лет и старше. Связано это с фактом отсутствия знаний подобной группы людей в ИТ-технологиях. Одним из самых распространенных преступлений с помощью хакерства является последующее мошенничество, где преступники апеллируют похищенными данными с целью извлечь финансовую выгоду. Это может быть вымогательство в форме шантажа, когда злоумышленник связывается с истинным владельцем данной информации, ставя в известность, что он может опубликовать данные в открытый доступ, или же может снять все деньги жертвы с банковского счета, предлагая свои условия. Зачастую этим условием является получение преступником определенной денежной суммы на счет, под обещание удалить похищенные данные и не совершать их опубликования в мировую сеть. Пожилые люди верят преступникам, отдавая им обозначенную сумму. Однако зачастую после получения этой суммы злоумышленники не останавливаются и продолжают вымогать денежные средства. Данный круговорот может продолжаться долгое время.

Привлечение повышенного внимания к данному виду преступлений необходимо. Информационное пространство не является безопасным, и хакеры могут взломать, похитить данные, с любого сервера, приложения или же компьютера.

Для противодействия киберпреступности, в частности хакерству, необходимо предпринимать определенные меры. Необходимо усовершенствовать сами серверы, уровень их безопасности, расставить так называемые «ловушки», где при попытке похищения данных или проникновения в базу данных без необходимого доступа – вычислялся IP-адрес данного лица. Необходимо также быстрое реагирование, чтобы специалисты могли вычислять местонахождение злоумышленника и передавать в уполномоченные службы. В таком случае, данные ведомства и спецслужбы должны оперативно среагировать и попытаться задержать преступника, дабы пресечь попытку похищения информации.

В XXI в. подобный вид преступлений лишь развивается, что освещается в СМИ с предупреждением о соблюдении мер безопасности в информационной среде, однако, как бы это ни было прискорбно признавать, все зависит от навыков преступника. На примере Сноудена можно сделать вывод, что человек может взломать самые сильно защищенные документы, базы данных, серверы, похитить информацию, не оставив следов. Также стоит отметить, что хакеры создают вредоносные программы, которые проникают в компьютер и также похищают данные.

Упомянем также одну из самых известных кибератака [5]. Предметом атаки стали правоохранительные органы и спецслужбы США. Хакеры из группировки Anonymous получили доступ к 269 Гб секретных данных правоохранительных органов и спецслужб США в виде более 1 млн файлов, что вызвало резонанс в СМИ и среди общественности. Также эта группа хакеров считается одной из самых опасных, поскольку их не останавливает ничего в их деятельности и никакие уровни секретности. Данная группировка похищала данные не только у правительства и спецслужб США, но и у других стран.

Исходя из вышесказанного, из приведенных выше фактов мы можем подвести итог. Им является острая необходимость в контроле за данным видом преступности, необходимости повышенного внимания и разработке различных программ для усиления безопасности серверов в мировой паутине. Объектом может стать не только обычный человек, но также и правительство, государственные органы, службы и ведомства. Преступность в IT-технологиях растет, а хакерство становится одним из самых главных видов совершения преступлений в информационной сфере, в сфере технологий. Если не обратить внимание на данную ситуацию сейчас, не предпринять меры, человечество перестанет ощущать безопасность в информационном пространстве, которое необходимо в XXI в. для выполнения рабочих или личных вопросов, деятельности.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.12.1996 № 63-ФЗ (ред. от 23.04.2019) // СПС «КонсультантПлюс».
2. Бутырская А. В., Шувалова А. М., Бубнова О. Ю. Актуальные вопросы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей // Российский следователь. 2022. № 12. С. 58–63.

3. Овсяков Д. А. Корыстные преступления против собственности с использованием информационно- телекоммуникационных сетей: вопросы квалификации : монография / под науч. ред. С. М. Кочои. М. : Проспект, 2023.
4. Комплексный анализ состояния преступности в Российской Федерации по итогам 2023 г. и ожидаемые тенденции ее развития / М. В. Гончарова, М. М. Бабаев, Р. В. Черкасов, Е. М. Тимошина, Г. Э. Бицадзе, К. С. Насуев, Г. Ф. Коимшиди, В. Г. Смирнов. М. : ФГКУ «ВНИИ МВД России», 2023.
5. Рычаго М. Е. Актуальные вопросы определения киберпространства и отражение киберпреступности в зеркале уголовной статистики / М. Е. Рычаго, Д. Н. Никитин // Пенитенциарное право: юридическая теория и правоприменительная практика. 2023. № 1 (35). С. 98–103.
6. Центральное разведывательное управление // Википедия. URL: https://ru.wikipedia.org/wiki/Центральное_разведывательное_управление.
7. Краткая характеристика состояния преступности в Российской Федерации за январь–март 2025 года // Министерство внутренних дел Российской Федерации. URL: <https://мвд.рф/reports/item/64450541/>.
8. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. М. : Московский университет МВД России имени В.Я. Кикотя, 2024. С. 35–37.
9. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. М. : Ай Пи Ар Медиа, 2025.
10. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. М. : Ай Пи Ар Медиа, 2025.
11. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. М. : Ай Пи Ар Медиа, 2025.
12. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стаценко [и др.]. Саратов : М. : Профобразование ; Ай Пи Ар Медиа, 2025.

*Амбросенкова Д. С.¹,
курсант Института-факультета подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

*Научный руководитель:
Константинов А. В.,
заместитель начальника кафедры
противодействия преступлениям
в сфере информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ПРОБЛЕМНЫЕ ВОПРОСЫ И ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ВЕБКАМ-ИНДУСТРИИ

Как показывает практика, на данный момент в России практика работы вебкам не урегулирована в рамках норм уголовного или какого-то другого законодательства. В то же время ранее были предприняты многочисленные попытки, направленные на урегулирование отношений в области сексуальных услуг. Так, принимались законопроекты «О государственной защите нравственности и физического здоровья граждан, об усилении контроля на обороте продукции сексуального характера», «О регулировании платных сексуальных услуг» [1].

На сегодняшний день вебкам-индустрия активно развивается, в большей степени с помощью цифровых технологий, а также онлайн-коммуникаций. В российском законодательстве данная сфера является проблемной, так как данный вопрос не урегулирован, существуют отдельные нормы, но их недостаточно.

Так как четкие законодательные нормы отсутствуют, в связи с этим возникают следующие негативные ситуации, такие как: Эксплуатация работников, вовлечение в индустрию несовершеннолетних, а также публикация в сеть Интернет. Поэтому возникает необходимость анализа и более детального исследования проблемных аспектов законодательства, а также разработка мер по его совершенствованию. На данный момент в Уголовном кодексе Российской Федерации нет отдельных статей, которые регулируют вебкам-студий и частных исполнителей, а в связи с этим и отсутствуют санкции за данное деяние.

В связи с этим возникает правовой вакуум. Рассматривая нормы уголовного права, вебкам-индустрию можно квалифицировать как ст. 127 УК РФ – эксплуатация человека. Однако данная статья применяется крайне редко, так как возникают проблемы в доказывании.

¹ © Амбросенкова Д. С., 2025.

Статья 240.1 УК РФ – вовлечение несовершеннолетних, но касается только отдельных действий, например, порнографии, но не вебкам-услуг, однако вышеуказанная деятельность в большинстве случаев непосредственно связана.

Статья 171 УК РФ – незаконное предпринимательство, так как многие студии, промышленяющие вебкам-индустрией для того, чтобы легализовать полученные денежные средства.

Известно о том, что модель может работать на индивидуальной основе или посредством вебкам агентства, которое обеспечивает не только техническую базу, но и материальную стабильную поддержку. Так, если модель заключает со студией контракт, то это значительно упрощает ее работу, так как управленческие функции, поиск и обустройство «места работы» для трансляций, создание учетной записи, активация аккаунта – всем этим занимаются специально обученные люди [2].

В российском законодательстве в принципе не существует понятие «вебкам», а также нет четко прописанных критерий, что относится к данной деятельности. В связи с этим возникает проблема квалификации. Суды могли рассматривать только собственные толкования, при этом не было допущено противоречий действующему законодательству.

Рассматривая докториальное толкование, то проблемность вопроса решали не через «вебкам», а через другую категорию – «распространение порнографических видеоматериалов в режиме реального времени с использованием сети Интернет», «участие в зрелищных мероприятиях порнографического характера в сети Интернет».

Анализирую нормы административного права, в частности ст. 6.11 КоАП – занятие проституцией. К данной статье деятельность вебкам-моделей, которая в большинстве случаев связана с оказанием интим-услуг. Но в данном случае усложняется процесс привлечения к ответственности организаторов, которые используют труд в принудительном порядке.

Стоит отметить, что многие вебкам студии работают через платформы иностранных государств, что, в свою очередь, осложняет контроль со стороны государства, а в некоторых случаях вовсе невозможен.

Распространены случаи:

- вымогательства денег у клиентов (ст. 163 УК РФ);
- несанкционированного распространения частных записей (ст.ст. 137, 138 УК РФ);
- обмана работников (невыплата заработной платы, ст. 145.1 УК РФ). Так как в вебкам индустрии задействованы, не только модели, но и операторы и другие лица, которые обеспечивают подключение связи.

В связи с этим, в данной статье предложены следующие меры для борьбы с вебкаи индустрией.

- во-первых, стоит закрепить определение «вебкам» в нормативной базе и выделить критерии под данную деятельность;
- дополнить в уголовный кодекс статьи, которые будут прямо регулировать вебкам-деятельность.

Например:

- «Незаконная организация вебкам-услуг» – для борьбы с нелегальными студиями;
- «Эксплуатация вебкам-моделей» – с учетом принудительного труда и психологического давления;
- «Вовлечение в вебкам-индустрию несовершеннолетних» – ужесточение наказаний за использование детей в онлайн-чатах.

Таким образом, вебкам-индустрия в Российской Федерации слабо урегулирована в законодательстве, что создает правовые пробелы и способствует совершению преступлений. Отсутствие нормативной база приводит к проблемам в квалификации деяний, связанных с эксплуатацией работников, вовлечением несовершеннолетних, мошенничеством и другими правонарушениями.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025) // СПС «КонсультантПлюс».
2. Аюпова Г. Ш. К вопросу о предмете преступления, предусмотренного статьей 242 УК РФ // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXIV междунар. науч.-практ. конф., Красноярск, 08–09 апреля 2021 года / отв. ред. Д. В. Ким. Красноярск : Сибир. юрид. ин-т Минва внутренних дел Российской Федерации, 2021.
3. Бадоян С. М. Криминалистические особенности установления лиц, совершивших распространение материалов с порнографическими изображениями несовершеннолетних в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2023. № 1 (25).
4. В Волгограде полицейскими пресечена деятельность организованной группы, занимавшейся изготовлением порнографических материалов // URL: <https://xn--b1aew.xn--plai/news/item/17170783/>.
5. Ваганова М. А., Копейка А. Н. Уголовно-правовое регулирование виртуальной проституции // Эволюция российского права. Екатеринбург, 2022.
6. Енгальчев В. Ф., Зайцева О. В. Выявление объектов детской порнографии в виртуальном пространстве посредством дешифровки наименований и тегов // Вестник Томского государственного университета. 2021. № 471.
7. Ильницкий А. С. Криминологические риски интимной коммуникации в сети Интернет // Гуманитарные, социально-экономические и общественные науки. 2021. № 9.
8. Полиция задержала восемь человек, которых обвинили в организации вебкам-студии в Красноярске. Им вменили создание преступного сообщества // URL: <https://tayga.info/165106>.
9. Хромов Е. В. Границы иных действий сексуального характера // Законность. 2021. № 1 (1035).
10. Шарапов Р. Д. Квалификация преступлений, связанных с незаконным оборотом порнографических материалов и предметов // Законность. 2021. № 8 (1042).

11. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
12. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
13. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. Москва : Ай Пи Ар Медиа, 2025.
14. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025.
15. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. 2024. № 5. С. 149–155.
16. Пушкарёв В. В. Осуществление уголовного преследования в досудебном производстве по уголовным делам о преступлениях, связанных с криптовалютами / В. В. Пушкарёв // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов, Москва, 30 марта 2023 года / сост. А. В. Константинов. Москва: Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя, 2023. С. 175–179.

Антюшина А. С.¹,
*курсант Института-факультета подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Рудин А. В.,
*доцент кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (НЕЙРОННЫХ СЕТЕЙ) В ДЕЯТЕЛЬНОСТИ ПОЛИЦИИ

В условиях стремительного развития цифровых технологий особое значение приобретает вопрос внедрения искусственного интеллекта (ИИ) в деятельность правоохранительных органов. Современные вызовы, стоящие перед полицией, требуют оперативной обработки большого объема информации, прогнозирования криминогенных рисков и обеспечения высокой эффективности в принятии решений. Одним из наиболее перспективных инструментов в этом направлении выступают нейронные сети – разновидность искусственного интеллекта, способная анализировать неструктурированные данные, выявлять закономерности и принимать решения на основе обучающей выборки.

Целью настоящего исследования является анализ возможностей, форм и ограничений применения нейронных сетей в системе органов внутренних дел Российской Федерации, а также оценка правовых и этических рисков, сопряженных с их использованием.

Нейронная сеть представляет собой математическую модель, вдохновленную структурой и работой биологических нейронов. Она состоит из слоев взаимосвязанных узлов (нейронов), каждый из которых выполняет простые вычисления, передает результат следующему слою и участвует в обучении системы.

Принципиальное отличие нейросетей от классических алгоритмов заключается в способности к самообучению на основе примеров, без необходимости детального программирования каждого шага, это делает их незаменимыми при анализе больших объемов неструктурированных данных: видео, аудио, текстов, изображений, паттернов поведения.

Наиболее перспективные направления использования нейронных сетей в деятельности органов правопорядка включают:

¹ © Антюшина А. С., 2025.

- видеоаналитика и распознавание лиц. Системы ИИ способны в режиме реального времени обрабатывать видеопотоки с уличных камер, распознавать лица, фиксировать подозрительное поведение. Такие технологии уже применяются

в мегаполисах для выявления разыскиваемых лиц и мониторинга массовых мероприятий;

- прогнозирование преступлений. На основе исторических данных об инцидентах, времени и месте совершения преступлений ИИ-модели могут выявлять закономерности и формировать прогностические карты (crime mapping), повышая эффективность патрулирования;

- обработка обращений граждан. Нейросети могут быть использованы для автоматизированной сортировки и предварительного анализа текстов обращений, жалоб и заявлений. Это способствует снижению нагрузки на сотрудников полиции и ускоряет реагирование;

- анализ интернет-контента. С помощью ИИ возможно выявление экстремистских публикаций, угроз массовой безопасности, фактов вербовки и пропаганды противоправной деятельности в социальных сетях;

- фоноскопический и лингвистический анализ. Системы ИИ применяются для идентификации личности по голосу, анализа речевых и текстовых сообщений, а также распознавания ложных заявлений.

Главные преимущества применения ИИ в деятельности полиции состоят в следующем:

1. Скорость и масштаб обработки информации. Нейросети способны анализировать огромные массивы данных в реальном времени, что невозможно при традиционных методах.

2. Объективность. При должной настройке системы ИИ исключают человеческий фактор, эмоциональные оценки, усталость, субъективность.

3. Повышение раскрываемости. За счет более точной аналитики и прогнозирования ИИ повышает вероятность выявления преступлений на ранней стадии.

4. Оптимизация ресурсов. Технологии ИИ позволяют сосредоточить усилия сотрудников на наиболее значимых направлениях, освободив их от рутинной работы.

Несмотря на очевидные преимущества, использование нейронных сетей в полицейской деятельности сопряжено с рядом ограничений. Во-первых, высока вероятность ошибок в интерпретации информации – алгоритмы могут допускать ложные срабатывания, особенно в условиях недостаточного обучения или при работе с данными низкого качества.

Во-вторых, стоит вопрос ответственности: кто несет ответственность за ошибку ИИ – разработчик, оператор системы или должностное лицо?

Кроме того, необходима правовая регламентация вопросов:

- допустимости применения ИИ в уголовно-процессуальных процедурах;
- хранения и обработки персональных данных граждан;
- недопущения дискриминации по признакам пола, расы, социального положения и иным критериям.

Особое внимание следует уделить обеспечению прозрачности алгоритмов принятия решений и сохранению права на апелляцию – гражданин должен понимать, по какой логике его действия были классифицированы системой как подозрительные.

Применение ИИ затрагивает фундаментальные права и свободы личности, включая право на неприкосновенность частной жизни и защиту персональных данных. Необходимым условием внедрения нейросетевых систем является соблюдение принципов:

- прозрачности. Алгоритмы и цели их применения должны быть открытыми для общественного контроля;
- соразмерности. Использование ИИ должно быть пропорционально поставленным целям обеспечения правопорядка;
- контролируемости. Важнейшим условием является наличие возможности у человека оспорить решение, принятое ИИ-системой.

Кроме того, необходимо формировать цифровую культуру у сотрудников полиции, обучать их принципам работы с ИИ, вопросам кибербезопасности и правовым рамкам использования новых технологий.

В Российской Федерации уже реализуются проекты по внедрению ИИ в деятельность правоохранительных органов. Например, разрабатываются системы интеллектуального анализа видеопотоков, проекты «Безопасный город» и «Цифровой участок», внедряются автоматизированные системы документооборота и распознавания номеров.

В перспективе возможно расширение применения ИИ в следующих направлениях:

- построение цифровых двойников преступных групп на основе анализа структурных связей;
- моделирование поведения потенциальных правонарушителей;
- предиктивная аналитика на базе интеграции данных МВД России, Росстата, Минздрава и других ведомств.

Однако успех этих инициатив напрямую зависит от нормативно-правового регулирования, общественного доверия, обеспечения кибербезопасности и подготовки кадров.

Искусственный интеллект и нейронные сети открывают новые горизонты для повышения эффективности работы полиции, позволяя своевременно выявлять угрозы, оперативно реагировать на инциденты и прогнозировать криминогенные ситуации. Однако технологии не могут заменить человеческий фактор, ответственность и профессиональное суждение. Они должны рассматриваться как вспомогательные инструменты, способные усилить аналитический потенциал полиции при соблюдении правовых и этических стандартов.

Развитие ИИ в правоохранительной сфере требует комплексного подхода: законодательной поддержки, научного сопровождения, технической экспертизы и постоянного диалога с гражданским обществом. Только при соблюдении этих условий нейросетевые технологии смогут стать эффективным и безопасным элементом цифровой трансформации полицейской службы.

Список литературы

1. Горбунов И. А. Искусственный интеллект в правоохранительной деятельности. М. : Юрайт, 2022.
2. Трофимов С. П. Этические аспекты внедрения ИИ в уголовное судопроизводство // Вестник уголовного права. 2023. № 2. С. 45–52.
3. Малышев В. Ю. Нейронные сети: алгоритмы, риски, перспективы. СПб. : Питер, 2021.
4. Официальный сайт МВД России. URL: <https://мвд.рф>.
5. OECD. Artificial Intelligence in Law Enforcement : Challenges and Recommendations. Paris : OECD Publishing, 2023.
6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
7. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
8. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. Москва : Ай Пи Ар Медиа, 2025.
9. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025.
10. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции. Москва : Московский университет МВД России имени В.Я. Кикотя, 2024. С. 35–37.
11. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. 2024. № 5. С. 149–155.

Байкова А. П.¹,
курсант Института-факультета подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Рудин А. В.,
доцент кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук

ПРОТИВОДЕЙСТВИЕ ДИСТАНЦИОННЫМ ХИЩЕНИЯМ: ПРОБЛЕМНЫЕ ВОПРОСЫ И ПУТИ РЕШЕНИЯ

В настоящее время информационно-телекоммуникационные технологии занимают значительное место в жизни каждого человека. В информационную среду переходит большое количество действий и операций, связанных с различными сферами деятельности, как личными и бытовыми, так и профессиональными. В числе таких действий и совершение различных финансовых операций, денежных переводов и иных манипуляций с принадлежащим гражданам имуществом, которое часто становится предметом преступных посягательств.

По данным прокуратуры г. Москвы за 2024 г. было зарегистрировано более 47 тыс. фактов совершения дистанционных хищений денежных средств у граждан, что составляет более 45 % от общего числа зарегистрированных преступлений против собственности [1]. При этом наиболее распространенными способами совершения данных деяний являются кража и мошенничество, ответственность за совершение которых устанавливается ст.ст. 158 и 159 УК РФ соответственно.

Кроме того, о значительном увеличении числа преступных посягательств на денежные средства как физических, так и юридических лиц свидетельствуют данные статистики Центрального банка Российской Федерации, согласно которым в 2024 г. объем операций без добровольного согласия клиентов увеличился по сравнению с 2023 г. на 74,36 %, а наибольшее количество фактов хищения денежных средств связано с использованием систем дистанционного банковского обслуживания, посредством преступного использования которых было похищено 9 602,57 млн рублей [2].

Рост масштабов компьютерной преступности отмечен в доктрине информационной безопасности Российской Федерации в качестве одной из важнейших

¹ © Байкова А. П., 2025.

информационных угроз [3]. В связи с этим борьба с преступлениями, совершаемыми с использованием информационных технологий, в том числе с дистанционными хищениями денежных средств, в настоящее время рассматривается как приоритетная задача государства.

Значительное место в системе противодействия дистанционному хищению денежных средств, на наш взгляд, должно уделяться совершенствованию уголовно-правовых мер борьбы с указанным видом преступлений.

В настоящее время Уголовным кодексом Российской Федерации предусмотрен только один случай, в котором совершение хищения путем использования информационных средств и методов считается наиболее опасной формой хищения и является квалифицированным составом преступления – кража с банковского счета или в отношении электронных денежных средств, ответственность за совершение которой предусмотрена п. «г» ч. 3 ст. 158 УК РФ.

Однако, необходимо отметить, что квалификации по указанному пункту ст. 158 УК РФ подлежат и деяния, связанные, например, с противоправным использованием банковских карт, принадлежащих гражданам, полученных, например, путем их хищения, что свидетельствует о том, что вопросы квалификации дистанционных хищений требуют дальнейшей проработки со стороны законодателя.

О наличии пробелов в данной области также свидетельствует отсутствие квалифицирующего признака, связанного с использованием дистанционных технологий, в составе преступления, предусмотренного ст. 159 УК РФ. Анализ судебной практики показал, что совершение хищения денежных средств путем совершения мошеннических действий с использованием сети Интернет, как правило, квалифицируются по ч. 3 или ч. 4 ст. 159 УК РФ, в зависимости от размера причиненного ущерба.

Так, Нагатинским районным судом г. Москвы признан виновным в совершении преступления, предусмотренного ч. 3 ст. 159 УК РФ, гражданин Притуленко М. Ю., который, действуя в составе группы с неустановленными следствием соучастниками, имитировал взлом аккаунта на портале «Госуслуги» потерпевшей А, после чего позвонил ей и сообщил о том, что на ее имя оформлены заявки на получение кредита в нескольких банках, в связи с чем для оформления апелляционной заявки и аннулирования всех кредитов ей необходимо оформить и получить кредит в банке на сумму 720 000 рублей, которые посредством курьера передать в сервисный центр портала «Госуслуги», что и было сделано потерпевшей [4]. За совершение указанного преступления Притуленко М. Ю. был осужден к двум годам лишения свободы условно, что, на наш взгляд, является недостаточно суровым наказанием за совершение хищения с использованием дистанционных технологий в крупном размере и может служить основанием для продолжения, осужденным преступной деятельности после исполнения назначенного наказания.

Таким образом, в действующем уголовном законе совершение хищения с использованием дистанционных технологий не выделено законодателем в качестве квалифицирующего признака кражи и мошенничества, что не соответствует современным условиям и существующей криминогенной обстановке в стране.

На наш взгляд, использование при совершении тайного хищения чужого имущества, а также при совершении мошеннических действий сети Интернет или других возможностей информационно-телекоммуникационного пространства должно быть выделено в качестве квалифицированных составов преступлений, предусмотренных ст.ст. 158 и 159 УК РФ, а также может быть включено в перечень отягчающих обстоятельств, содержащийся в ст. 63 УК РФ, что позволит ужесточить назначаемое за совершение указанных преступлений наказание и повысить эффективность уголовно-правовых средств противодействия данным преступлениям.

Важную роль в противодействии дистанционным хищениям играет эффективность процессов раскрытия и расследования рассматриваемых преступлений. В настоящее время существует ряд сложностей, с которыми сталкиваются субъекты данной деятельности.

Одной из проблем, возникающих в ходе раскрытия и расследования дистанционных хищений, является вопрос, связанный с определением места совершения преступного деяния, которое является важнейшим обстоятельством, подлежащим доказыванию по уголовному делу, а также является определяющим в решении ряда процессуальных вопросов, в том числе связанных с местом производства предварительного расследования.

Аналогичной точки зрения придерживается и Митрофанов Р. А., который отмечает, что характерной особенностью дистанционных хищений является отсутствие непосредственного контакта злоумышленника и жертвы. Это приводит к фактическому несовпадению места непосредственного совершения преступления с местом наступления преступных последствий, что вызывает массу сложностей в ходе расследования [5, с. 97].

Для решения указанной проблемы, на наш взгляд, необходимо включить в Постановления Пленума Верховного Суда РФ, регламентирующие вопросы применения ст.ст. 158 и 159 УК РФ положений о том, что местом совершения хищения, совершенного с использованием дистанционных технологий, может быть признано место нахождения устройства, с помощью которого совершены преступные действия, направленные на дистанционное хищение (при наличии возможности его установления), либо место наступления преступных последствий.

Помимо этого, большое значение в процессе расследования дистанционных хищений имеют процессы фиксации и изъятия доказательств, которые содержатся в электронной среде. В настоящее время идет процесс внесения в уголовно-процессуальное законодательство изменений, определяющих порядок работы с цифровыми следами. Однако указанный процесс не завершен, в связи с чем в процессе расследования нередко возникают проблемы, связанные с получением таких доказательств.

В частности, одной из таких проблем является необходимость привлечения к участию в следственных действиях специалиста, обладающего специальными познаниями в сфере информационно-телекоммуникационных технологий.

Колычева А. Н. отмечает, что привлекаемые специалисты при расследовании рассматриваемых преступлений играют особую роль [6, с. 294]. В частности, они должны оказывать следователю содействие в процессе обнаружения, фиксации

и изъятия цифровых следов, осмотре технических средств, подготовке к следственным действиям, в том числе допросам технических специалистов, назначении экспертиз, а также консультационную помощь, связанную с разъяснением специфической терминологии при изучении технической документации.

Однако в практике следственной деятельности приглашение специалиста в данной области вызывает определенные сложности, связанные с тем, что сотрудники экспертно-криминалистических центров и других подразделений правоохранительных органов не всегда обладают необходимым уровнем подготовки для оказания квалифицированной помощи субъектам расследования, а поиск специалистов в других организациях требует значительных временных и материальных затрат.

В связи с этим важнейшим направлением противодействия дистанционным хищениям является подготовка квалифицированных специалистов, обладающих достаточным уровнем знаний в области информационно-телекоммуникационных технологий, который позволит осуществлять оперативное обнаружение и грамотные фиксацию и изъятие цифровых следов дистанционного мошенничества, позволяющие эффективно вести процесс расследования данных преступлений.

Отдельно необходимо отметить, что процессы противодействия дистанционным хищениям тесно связаны с повышением уровня защиты персональных данных граждан, содержащихся в информационной среде, а также на различных электронных платформах, на которых возможно размещение денежных средств или совершение банковских операций, в том числе приложений «Мобильный банк» и различных электронных платежных систем. Пивнева Л. А. отмечает, что сегодня уровень защиты информационного пространства находится на недостаточно высоком уровне [7, с. 425]. В связи с этим необходимо совершенствовать существующие механизмы информационной безопасности.

В настоящее время в качестве наиболее простого и эффективного способа защиты выступает установка системы двухфакторной аутентификации при совершении денежных операций, которая, на наш взгляд, должна устанавливаться на любую сумму для всех клиентов банков. Помимо этого, эффективным средством противодействия дистанционным хищениям станет и введенная в начале 2025 г. возможность установления самозапрета на заключение договоров потребительских кредитов (займов). При этом необходимо активно информировать население о наличии такой возможности и позитивных последствиях ее использования.

Таким образом, противодействие дистанционным хищениям является важнейшим направлением деятельности как правоохранительных органов, так и всех органов и организаций, связанных с предоставлением гражданам возможности совершать денежные операции в электронной среде.

Список литературы

1. Прокуратура города Москвы. URL: https://epp.genproc.gov.ru/web/proc_77/mass-media/news?item=99956085.
2. Банк России. URL: https://cbr.ru/analytics/ib/operations_survey/2024/.

3. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».
4. Приговор № 1-1179/2024 Нагатинского районного суда г. Москвы от 28.12.2024 // Официальный портал Судов общей юрисдикции города Москвы. URL: <https://mos-gorsud.ru>.
5. Митрофанов Р. А. Дистанционные хищения: теоретические и практические вопросы // Ученые записки. 2022. № 1 (41). С. 95–99.
6. Колычева А. Н. Дистанционные способы хищения: разновидности и отдельные аспекты противодействия // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2024. Т. 10 (76). № 1. С. 291–295.
7. Пивнева Л. В. Дистанционное мошенничество: современные способы совершения преступления и проблемы раскрытия // Инновационный потенциал развития общества: взгляд молодых ученых: Сборник научных статей 4-й Всероссийской научной конференции перспективных разработок. Курск: ЗАО «Университетская книга», 2023. С. 425–428.
8. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
9. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
10. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. Москва : Ай Пи Ар Медиа, 2025.
11. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025.
12. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции. Москва : Московский университет МВД России имени В.Я. Кикотя, 2024. С. 35–37.
13. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. 2024. № 5. С. 149–155.

Баканов Н. А.¹,
слушатель Института-факультета подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Рудин А. В.,
доцент кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук

ИСПОЛЬЗОВАНИЕ ПОМОЩИ НАСЕЛЕНИЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПОМОЩЬЮ ИНФОРМАЦИОННЫХ- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

С каждым годом число преступлений совершенных с использованием информационно-телекоммуникационных технологий (далее – ИТТ) растет. Только за 2024 г., по данным МВД России, было совершено чуть более 765 тыс. преступлений, совершенных с использованием ИТТ, что является 40 % от всех преступлений [3]. Данная статистика говорит нам о том, что сегодня, во времена информационных технологий, необходимы новшества в сфере правоохранительной системы, которая должна адаптироваться и меняться под нынешнюю ситуацию.

Безусловно, со временем все меняется, но что остается неизменным – это взаимодействие между людьми и государством, в котором они живут. Само взаимодействие играет огромное значение в нашей жизни. Оно способствует развитию социально важных навыков, эмпатии, обмену информацией, формированию социальной поддержки и солидарности. В общем, взаимодействие между людьми помогает нам быть более эмоционально зрелыми, образованными, поддерживать здоровые отношения и чувствовать себя частью сообщества.

Взаимодействие с ОВД также является очень важным аспектом в жизни общества. Можно сказать, что это взаимодействие является неотъемлемой частью эффективной системы обеспечения общественной безопасности. Сегодня с каждым днем преступность растет, и не всегда предоставляется возможность предотвратить данные преступления.

Сегодня, в условиях информатизации преступлений, организация взаимодействия общества с полицией требует проработки и изменений, которые помогут бороться с преступлениями, совершенными с использованием ИТТ, эффектив-

¹ © Баканов Н. А., 2025.

ней. Отрицательный опыт взаимодействия с правоохранительными органами играет плохую роль в противодействии преступности, в частности в выявлении и предотвращении преступных действий. Данный опыт, может быть связан с неграмотной организацией взаимодействия ОВД с обществом, что порождает недоверие полиции среди населения. Это указывает на то, что тема работы очень актуальна и требует конкретного изучения.

Обращаясь к теоретическим аспектам данной темы, мы можем сказать, что определение информационно-телекоммуникационных технологий официально нигде не закреплено, но если мы обратимся к Федеральному закону от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», а именно к ст. 2, в которой указано, что под информационно-телекоммуникационной сетью, мы понимаем – «технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники» [6], то будет ясно, что информационно-телекоммуникационными технологиями являются – «совокупность методов, процессов и устройств, позволяющих получать, собирать, накапливать, хранить, обрабатывать и передавать информацию, закодированную в цифровом виде или существующую в аналоговом виде» [5]. Главное в данном определении то, что в нашем случае мы имеем дело с такими процессами, которые сложно выявить и еще сложнее отследить.

Если перейти к непосредственному взаимодействию населения и ОВД, то в данном случае взаимодействие представляет собой деятельность населения и ОВД, которая объединена одной целью, местом, временем применения сил и средств для выполнения определенных задач [8, с. 37–46].

Мы понимаем, что взаимодействие населения с ОВД может проявляться по-разному, т. е. в различных формах.

В научной литературе существует много различных подходов к разграничению форм взаимодействия, но мы будем придерживаться следующей.

Первая форма – это совместно проводимый анализ состояния охраны общественного порядка и общественной безопасности. Примером может служить выступления участкового уполномоченного полиции перед населением, где он освещает результаты работы ОУУП и ПНД своего отдела, также может затронуть тему противодействия тому или иному преступлению (правонарушению), которое преобладает на его участке, его профилактики и бдительности граждан.

Следующая форма взаимодействия – это разработка совместных мероприятий по профилактике противоправных деяний. Примером являются агитация, семинары и лекции на данную тему в различных учреждениях. Также это своевременное сообщение о странном или подозрительном поведении граждан.

Третья форма – это непосредственное обучение и инструктаж участников общественных объединений методам и формам правоохранительной деятельности. В данном случае сотрудники полиции обучают участников правовым основам, принципам участия, рассказывают о правах и обязанностях членов общественных объединений. Также докладывают об особенностях охраны общественного порядка и о порядке взаимодействия всех участников.

Четвертая форма – это совместное с сотрудниками обеспечение порядка на административных участках и профилактика противоправных деяний среди лиц, не достигших совершеннолетия. Мы понимаем, что это уже непосредственное действие, которое направлено на единую цель. Также к данной форме нередко относят и совместное патрулирование с нарядами ППС [7].

Рассматривая НПА, связанных с взаимодействием ОВД и населения, то мы можем обратиться к Федеральному закону № 3 «О полиции» от 07.02.2011, в котором мы можем наблюдать основные положения, которые как раз и определяют правовые основы взаимодействия населения с ОВД. В частности, данный закон регулирует полномочия полиции и устанавливает процедуры обращения граждан. Согласно закону, полиция обязана принимать заявления от граждан и проводить проверку по данному факту, а также информировать заявителей о ходе «дела». Более того в главные принципы деятельности полиции входят такие принципы, как: «открытость и публичность», «общественное доверие и поддержка граждан», «взаимодействие и сотрудничество». Все эти принципы уже говорят о том, что полиция стремится к правильному и эффективному взаимодействию с гражданами, ведь от этого и зависит их безопасность.

Также хочется упомянуть Федеральный закон «Об участии граждан в охране общественного порядка» от 02.04.2014 № 44. Данный нормативный правовой акт регулирует вопросы участия граждан в обеспечении общественной безопасности и поддержании общественного порядка. Закон предусматривает возможность активного участия граждан в охране общественного порядка, сотрудничества с правоохранительными органами и повышения эффективности преступно-правовой деятельности. Он устанавливает правовые основы для такого участия, а также определяет права и обязанности граждан, средства и методы их участия. В соответствии с законом граждане могут принимать участие в охране общественного порядка посредством надзора, информирования правоохранительных органов о преступлениях и правонарушениях, оказания помощи в задержании правонарушителей, а также посредством сотрудничества с правоохранительными органами. Федеральный закон № 44 содействует формированию эффективной системы взаимодействия между гражданами и правоохранительными органами, что способствует повышению уровня общественной безопасности и защите прав граждан [4, с. 280–283].

Переходя к практическому аспекту работы, хочется отметить, что взаимодействие граждан с ОВД, которое должно помочь бороться с преступлениями, совершенными с использованием ИТТ, необходимо строить на доверии и повышении «имиджа» полиции. Ведь, по данным Всероссийского центра изучения общественного мнения, начиная с 1992 г. уровень доверия российского населения ОВД не превышал 46 %, что является неутешительной статистикой [2, с. 144–150].

При анализе потребностей общества и отношения к различным вещам, становится очевидным огромное внимание людей к мессенджерам. Данный продукт особенно стал популярным в период пандемии, где люди попросту не могли общаться в живую. Более того, в наше время без мессенджеров невозможно представить нашу жизнь, они влияют не только на нашу повседневную жизнь, но и на культуру и определенные устои. Согласно исследованию ВЦИОМ, 86 %

россиян, пользующихся хотя бы одной социальной сетью или мессенджером, проводят в них время практически ежедневно; среди молодежи 18–34 лет доля ежедневных пользователей близка к абсолютной (18–24 лет – 92 %, 25–34 лет – 94 %). Также регулярные пользователи социальных сетей и мессенджеров в среднем тратят на них 272 минуты или же 4,5 часа в день [1]. Данная статистика говорит сама за себя и является тем камнем преткновения во взаимодействии государства с населением, особенно с молодым населением.

Зачастую, оперативность в расследовании преступлений, совершенных с использованием ИТТ играет огромную роль. Мы считаем, что ОВД не хватает именно внедрение в свою деятельность большего числа электронных сервисов и онлайн-платформ, через которые граждане смогли бы взаимодействовать с органом исполнительной власти в быстром формате. Стоит отметить, что данные шаги уже предпринимались ОВД, но их недостаточно. Разработка электронных сервисов и онлайн-платформ позволит гражданам в привычной среде подавать заявления, получать информацию о новых преступных схемах и в общем быстро взаимодействовать с полицией. Один сотрудник или даже группа, которая сможет грамотно и с пользой ввести данную страницу в мессенджерах или соцсетях, сможет увеличить эффективность своей работы. Также благодаря этому, доверие граждан тоже возрастет, так как данное изменение будет демонстрировать готовность полиции модернизироваться и ближе взаимодействовать с гражданами. Может возникнуть вопрос в какой форме граждане смогут подать заявление о происшествии? Данный пункт будет регулироваться как простое электронная подача заявления, согласно Федерального закона от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и приказу МВД России от 12 сентября 2013 г. № 707 «Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации». А именно «При заполнении формы обращения вам в обязательном порядке следует указать: фамилию, имя, отчество (при наличии), адрес электронной почты для направления ответа или уведомления, суть обращения. Также вы вправе приложить к обращению необходимые документы и материалы в электронной форме». Поступившие обращения регистрируются в трехдневный срок и рассматриваются в течение 30 дней со дня регистрации. При необходимости, срок рассмотрения может быть продлен не более чем на 30 дней, о чем направляется уведомление также в мессенджере. Отметим, что все равно, в данном случае, особое значение будет играть оперативность принятия и обработки сообщений, особенно о преступлениях, совершенных с использованием ИТТ.

Также мы считаем важным, в борьбе с преступлениями, совершенными с использованием ИТТ, расширить программы социального партнерства. Общество, а в частности граждане и организации смогут разрабатывать свои проекты по улучшению деятельности полиции, более того – это актуально в сфере информационной безопасности. Каждый человек, который действительно хочет помочь государству бороться с преступлениями, сможет быть полезен. Соответственно, комиссия из числа сотрудников ОВД сможет принимать и утверждать на конкурсной основе некоторые проекты, которые будут воплощены в жизнь

это также покажет настрой полиции менять в лучшую сторону и будет способствовать доверительному отношению населения.

Также нельзя не сказать о важной сфере, где необходимы изменения – это образование. Для улучшения взаимодействия с населением необходимо развивать программы образования и информирования о правах и обязанностей граждан, а также о деятельности ОВД. Стоит постараться сформировать правильное отношение нового поколения к закону и его соблюдению. Также данное информирование должно происходить на уровне с возрастным восприятием каждого человека, мы имеем в виду то, что для подростков подойдет один подход, а для детей дошкольного возраста совсем другой. Все это также должна учитывать полиция при разработки данных программ. Отметим, что данное информирование предназначено для всех возрастных групп населения.

Мы считаем, что данные предложения безусловно должны сказаться в лучшую сторону в борьбе с преступлениями, совершенными с использованием ИТТ, более того все меры необходимо вводить на длительную перспективу, все это должно сопровождаться цифровизацией и информатизацией ОВД, так как полиция должна быть современной и понятной людям, которые выросли на различных гаджетах и интернете. Более того, сотрудники также должны быть «подкованы» и работать с информационными ресурсами на «ты».

Список литературы

1. ВЦИОМ Социальные сети и мессенджеры: вовлеченность и предпочтения // URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-messendzhery-vovlechennost-i-predpochtenija>.
2. Зуева О. В., Демидов Н. Н. Доверие граждан к полиции в современной России: актуальное состояние и анализ факторов // Вестник Московского государственного лингвистического университета. Общественные науки. 2022. № 2.
3. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2024 года // URL: <https://мвд.рф/reports/item/60248328/>.
4. Потапенкова И. В. О проблемных вопросах реализации Федерального закона от 2 апреля 2014 г. № 44-ФЗ «Об участии граждан в охране общественного порядка» // Вестник Московского университета МВД России. 2014. № 10.
5. Телекоммуникационные технологии // URL: <https://www.sviaz-expo.ru/ru/ui/17142/>.
6. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2025) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/.
7. Формы взаимодействия полиции с общественными объединениями, организациями, учреждениями и гражданами 2020 г. // URL: https://studopedia.ru/26_102609_formi-vzaimodeystviya-politsii-s-obshchestvennimi-ob-edineniyami-organizatsiyami-uchrezhdeniyami-i-grazhdanami.html.

8. Щербаков О. Н., Диянич В. Ю. Взаимодействие органов внутренних дел (полиции) с гражданами по вопросам охраны общественного порядка // Полицейская деятельность. 2019. № 5.

9. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. 2024. № 5. С. 149–155.

10. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.

11. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.

12. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. Москва : Ай Пи Ар Медиа, 2025.

13. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025.

Белякова А. А.¹,
курсант Института-факультета подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Михайленко Н. В.,
доцент кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

РИСКИ РЕАЛЬНОЙ ЛИЧНОСТИ ПОД ВОЗДЕЙСТВИЕМ ЦИФРОВИЗАЦИИ И ЦИФРОВОЙ ЛИЧНОСТИ

По мере распространения Интернета «цифровая личность» стала важной социальной и политической темой. Потребность и желание самовыражения – великий дар общения, и общество должно его принять. Но при этом цифровая личность не должна подвергать риску реальную личность человека. По меньшей мере существует три аспекта, которыми характеризуется любая цифровая личность: индивидуальный IP-адрес [1], личная информация и логины, цифровые подписи и метаданные. Необходимо отметить, что они имеют мало общего с тем, кто вы есть как реальная личность или даже ваша онлайн-личность, если вторая отличается от первой. Это просто набор данных, который показывает, как, откуда и когда вы выходите в Интернет.

Утрата этих данных поставит под угрозу вашу репутацию в случае их злонамеренной кражи и неправомерного использования, а также может нарушить все другие аспекты вашей жизни, особенно сейчас, когда большинство связей, которые мы устанавливаем, находятся в Интернете. К счастью, есть решения. Например, с хорошей виртуальной частной сетью, такой как Le VPN, вы можете замаскировать свой IP-адрес и удалить большинство следов, которые вы оставляете, когда речь идет о метаданных. А немного потренировавшись, вы сможете стать по-настоящему невидимым для шпионов и хакеров.

То, что мы раньше считали общим виртуальным пространством, теперь официально названо метавселенной [2]. Но та информация, которой мы там делимся добровольно, гораздо важнее, чем большинство технологических гигантов могут добыть.

Любой и каждый заслуживает подключения к миру в целом через Интернет, но, как и в настоящей жизни, виртуальная реальность часто бывает грязной

¹ © Белякова А. А., 2025.

и враждебной. В результате, некоторая приватная информация интернет-пользователей может стать открытой для тех, кто хочет исследовать.

Кроме того, для тех, кто устанавливает большую часть своих связей посредством Интернета, а это все большее число людей, перенесенный виртуальный стресс превратится в реальный. Любое преследование и агрессия в сети будут ощущаться так же, как если бы эти люди присутствовали рядом с вами в реальной жизни. Вот почему вы всегда должны держать три части своей личности разделенными. Ваша социальная личность – это не то же самое, что ваша цифровая личность и ваша реальная личность. Знание того, как защитить себя мысленно и в цифровом виде, станет началом осознанной защищенной жизни. Социальная идентичность сложнее, и защита ее – вопрос скорее философский, чем технический.

Но, что вы всегда должны иметь в виду: Интернет – пространство свободы. Вы можете раскрываться столько, сколько хотите, и не обращать внимания на то, как другие реагируют на ваш образ жизни или действия, если вы никому не причиняете вреда. Мы же понимаем, что невозможно заставить других вести себя прилично или уважать нашу личность, и мы не можем ожидать или требовать этого от аморфной толпы, которой является Интернет.

Защитив свою цифровую личность с помощью VPN премиум-класса, такой как Le VPN, вы можете помешать людям взломать вас, отследить или украсть ваши данные. Таким образом, вы можете сосредоточиться на развитии своей реальной и социальной личности. Если вам важно быть признанным обществом, делайте себя, как социальную личность, сами, не расталкивая других и никогда не позволяя другим толкать вас.

Существует слой философов и ученых, которые предсказывают слияние человека и машины в ближайшем будущем. По их мнению, человеческие тела в своем первозданном виде приспособлены исключительно для недолгой жизни на нашей родной планете. Но как в таком случае продлить само существование нашей цивилизации, особенно ввиду многочисленных угроз, стоящих перед человечеством? Ответ, вероятно, кроется в объединении машины и человека. Постоянно растущая скорость развития технологий и нейробиологии в сочетании с созданием суперкомпьютеров, усовершенствованных частей тела и искусственных конечностей прокладывает путь к слиянию человека и машины. Современный человек идет целенаправленно к вырождению. Он отказывается от собственной природы, больше того – человек идет против нее. Реальность подменяется виртуальностью, тело подвергается модификациям, а разум, который создал нашу цивилизацию, постепенно трансформируется в искусственный интеллект.

Следующим шагом, надо полагать, будет возможное слияние искусственного интеллекта и человека в одно целое. Со временем искусственные органы вытеснят более долговечные бионические части тела. Откроется второй информационный канал, который, минуя органы чувств, будет напрямую поступать в «прокачанный» мозг. Эпоха старого человечества закончится, и начнется новая эра развития разумной жизни. Однако такие установки скрывают реальную опасность появления непрогнозируемых последствий, вызывая этим естественную тревогу о будущем человека, исторических судьбах человечества.

Несмотря на важность цифровизации личности человека в условиях современности, необходимо учитывать и то факт, что существуют определенные риски, связанные с ее развитием. Человек, как и любое живое существо, подвергается стрессу, а также физическим травмам как в быту, так и со стороны общества, рассматриваемая тема позволяет в будущем избегать подобного рода проблем, а также устранять их полностью путем создания искусственных частей человеческого тела и замещения ими настоящие, живые органы, как на нейронном уровне, так и на двигательном. Данный вопрос становится основополагающим в области развития человеческого рода, такие концепции позволят воспроизвести «сверхчеловека», который станет новейшей вехой человечества.

Список литературы

1. Овчинников А. И. и др. Цифровая безопасность личности, общества и государства в условиях глобализации: юридические механизмы обеспечения. Обзор сессии в рамках ПМЮФ 2019 г. // Вестник юридического факультета Южного федерального университета. 2019. Т. 6. №. 2. С. 111–122.
2. Филимонова Е. А., Бондаренко В. С. Цифровая безопасность личности // Социальные институты в цифровой среде. 2020. С. 465–469.
3. Грачева Ю. В. Цифровые технологии и безопасность личности // Криминалист. 2019. №. 1. С. 24–27.
4. Попова Д. А. Цифровая личность как центральный элемент межперсонального интернет-дискурса // Вестник Бурятского государственного университета. Язык. Литература. Культура. 2019. №. 2. С. 87–91.
5. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
6. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
7. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. Москва : Ай Пи Ар Медиа, 2025.
8. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025.
9. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. Москва : Московский университет МВД России имени В.Я. Кикотя, 2024.
10. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. 2024. № 5. С. 149–155.
11. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. 2023. № 4. С. 88–92.

Бойко И. В.¹,
курсант факультета подготовки
сотрудников для оперативных
подразделений полиции
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Апаев И. Х.,
старший преподаватель кафедры
оперативно-разыскной деятельности
и специальной техники
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук

ОПЕРАТИВНО-РАЗЫСКОЕ ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВАМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

В последние годы мир наблюдает стремительное развитие цифровых технологий, которые проникают во все сферы жизни общества. Не остаются в стороне и финансовые операции, где в качестве нововведения выступают криптовалюты. Этот феномен привлекает внимание не только инвесторов и предпринимателей, но и мошенников, видящих в нем новые возможности для совершения преступлений. Противодействие мошенничеству, совершаемому с использованием криптовалют, становится актуальной задачей для оперативных подразделений органов внутренних дел Российской Федерации [2].

Сложность борьбы с такого рода преступлениями заключается в анонимности транзакций и международном характере деятельности, что требует от правоохранительных органов не только специфических знаний и навыков, но и тесного международного взаимодействия. Наряду с этим необходимо постоянное обновление законодательной базы, адаптирующейся к быстро меняющемуся цифровому миру. Оперативные подразделения органов внутренних дел играют ключевую роль в противодействии мошенничествам, совершаемым через криптовалюты [1]. С учетом анонимности и трансграничного характера криптовалютных операций, это представляет значительные трудности для идентификации злоумышленников и возврата украденных средств. Для эффективного решения данных задач требуется высокий уровень квалификации сотрудников, знание особенностей блокчейн-технологий и владение инструментарием для отслеживания цифровых транзакций.

В России наблюдается рост мошенничеств, связанных с криптовалютами. Преступники активно используют анонимность и сложность отслеживания операций в блокчейне. Характерными схемами являются фишинг, с целью кражи

¹ © Бойко И. В., 2025.

данных для доступа к криптокошелькам, и пирамиды, привлекающие вложения под предлогом высоких доходов. Из-за отсутствия строго регулирования крипторынка оперативные подразделения сталкиваются с вызовами в идентификации и преследовании злоумышленников [3].

Одной из ключевых проблем, с которой сталкиваются оперативные подразделения при противодействии криптовалютным мошенничествам, является высокая анонимность транзакций. Это усложняет идентификацию участников мошеннических схем. Кроме того, отсутствие единой международной правовой базы для регулирования операций с криптовалютами приводит к трудностям в проведении международных расследований. Технологическая сложность и постоянное развитие методов кибермошенничества требуют от оперативников не только специализированных знаний в области криптовалют, но и постоянного обновления их навыков.

Одной из ключевых задач оперативных подразделений органов внутренних дел РФ является обнаружение и раскрытие мошеннических схем, включающих использование криптовалют. Для эффективной работы в этом направлении применяются различные современные методы и инструменты. Среди них – анализ блокчейн-транзакций, который позволяет отслеживать перемещение средств и выявлять подозрительные операции. Активно используются и сервисы для деанонимизации кошельков, что способствует идентификации лиц, причастных к мошенничеству. В арсенале также нейросети и искусственный интеллект для анализа больших объемов данных и выявления закономерностей, характерных для мошеннической деятельности. Эти методы служат мощной основой для борьбы с криптовалютными аферами.

В перспективе развития работы оперативных подразделений по борьбе с криптовалютным мошенничеством в России ключевым аспектом станет усиление межведомственного взаимодействия и обмена информацией. Применение технологий блокчейн для отслеживания транзакций и анализа данных поможет выявлять и пресекать мошеннические операции на ранних стадиях. Разработка и внедрение инновационных методов расследования, а также повышение уровня квалификации сотрудников станут ключевыми задачами. Создание специализированных подразделений и использование искусственного интеллекта для анализа киберпространства обеспечат опережающее реагирование на новые виды мошенничеств, связанные с криптовалютами.

Сложность борьбы с криптовалютными мошенниками заключается в анонимности и трансграничном характере данных операций, что ставит под вопрос эффективность традиционных методов расследования [4]. В этом контексте, актуальность разработки и внедрения инновационных технологий и международного сотрудничества в этой сфере становится очевидной.

С развитием цифровых технологий и популяризацией криптовалют, формы кибермошенничества становятся все более сложными и разнообразными. Оперативные подразделения органов внутренних дел сталкиваются с вызовами в идентификации и преследовании злоумышленников, ведь криптовалютные транзакции обладают высокой степенью анонимности. Это усложняет процесс выявления виновных лиц и возвращения средств пострадавшим. Кроме того, недостаток

четко выраженного законодательства в сфере регулирования цифровых валют значительно ограничивает возможности правоохранительных органов по борьбе с таким видом преступлений.

Оперативные подразделения органов внутренних дел играют ключевую роль в выявлении и пресечении финансовых преступлений, связанных с использованием криптовалют. В условиях активного роста криптовалютного рынка мошенники нашли в нем плодородную почву для совершения преступлений: от отмывания денег до финансирования терроризма. Помимо традиционных методов расследования, такая деятельность требует от сотрудников глубоких знаний кибербезопасности и блокчейн-технологий для отслеживания транзакций в децентрализованных сетях [5]. Эффективное противодействие таким преступлениям невозможно без внедрения новейших технологических решений и разработки международного сотрудничества для обмена опытом и информацией.

Оперативные подразделения органов внутренних дел Российской Федерации сталкиваются с технологическими вызовами при расследовании мошенничеств, использующих криптовалюты. Анонимность и децентрализация криптовалютных транзакций осложняют выявление злоумышленников и восстановление средств жертв. В ответ на это, разрабатываются инновационные методы и инструменты. Применение блокчейн-аналитики, развитие способов прослеживания транзакций и сотрудничество с криптоплатформами позволяют эффективнее идентифицировать подозреваемых и блокировать мошеннические активы. Эти меры помогают минимизировать риски и защитить граждан.

Эффективное противодействие мошенничествам, совершаемым с использованием криптовалют, требует тесного сотрудничества оперативных подразделений органов внутренних дел с экспертами в области кибербезопасности. Взаимодействие этих групп способствует обмену знаниями и информацией, что крайне важно для быстрого выявления и предотвращения финансовых преступлений. Обучение сотрудников органов внутренних дел особенностям технологий блокчейн и криптовалют позволяет повысить их компетенции в данной области, а также улучшить межведомственное взаимодействие.

Развитие технологий в сфере криминалистики и кибербезопасности открывает новые горизонты для оперативных подразделений России в борьбе с киберпреступлениями. Экспертиза блокчейна, усовершенствованный анализ транзакций и использование искусственного интеллекта для отслеживания схем мошенничества с криптовалютами становятся ключевыми направлениями. Создание специализированных подразделений и обучение персонала на курсах по кибербезопасности повысят эффективность работы. Взаимодействие с международными организациями и обмен данными также способствует пресечению кибермошенничеств.

Список литературы

1. Антонов И. А. Начальный этап раскрытия и расследования мошенничества, совершенного с использованием средств сотовой связи, и развитие технико-кри-

миналистического обеспечения деятельности органов предварительного расследования // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности : сборник научных статей по материалам международной научно-практической конференции, Москва, 26 мая 2023 года. Часть 2. М. : Академия управления Министерства внутренних дел Российской Федерации, 2023. С. 13–22.

2. Гумаров И. А. Некоторые проблемы организации работы оперативных подразделений органов внутренних дел по противодействию мошенничествам общеуголовной направленности / И. А. Гумаров, В. Ф. Саэтгараев // Вестник Казанского юридического института МВД России. 2018. № 2 (32). С. 223–230.

3. Дорофеев К. И. Особенности организации расследования мошенничеств, совершенных дистанционным способом // Академическая мысль. 2019. № 4 (9). С. 55–61.

4. Озеров К. И. Использование современных цифровых технологий в оперативно-розыскном противодействии IT-мошенничествам в призме обеспечения национальной безопасности // Актуальные вопросы обеспечения национальной безопасности: материалы международной научно-практической конференции, Санкт-Петербург, 30 ноября 2022 года. Москва : Московская академия Следственного комитета Российской Федерации, 2023. С. 82–86.

5. Шерешова С. А. Оперативно-розыскное противодействие мошенничествам в сфере компьютерной информации // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: Сборник материалов конференции, Воронеж, 28 мая 2023 года. Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2023. С. 346–348.

Брюзгин А. И.¹,
курсант Института-факультета подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
заместитель начальника кафедры
противодействия преступлениям
в сфере информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ЗАЩИТА ИНТЕРНЕТА ВЕЩЕЙ (IOT) ОТ КИБЕРАТАК

Интернет вещей (IoT) представляет собой совокупность сетевых устройств, объединенных для обмена данными и обеспечения взаимодействия между объектами в реальном времени. Быстрое развитие IoT-технологий в различных секторах экономики, включая энергетику, транспорт, здравоохранение и промышленность, приводит к существенному усложнению вопросов информационной безопасности. Рост объема передаваемой данных, увеличение числа подключенных устройств и разнообразие функционала требуют пересмотра традиционных мер защиты информации.

Современные исследования в области кибербезопасности указывают на значительное количество уязвимостей IoT-систем, что может привести к нарушению работы критической инфраструктуры и нанесению экономического ущерба. В данной статье проводится анализ нормативно-правовой базы Российской Федерации (далее – РФ) в области защиты информационной инфраструктуры, рассматриваются современные угрозы и предлагаются методы защиты IoT-устройств от кибератак.

Правовое регулирование информационной безопасности в РФ основывается на ряде федеральных законов и нормативных актов. В числе основных документов следует отметить:

1. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ, который устанавливает правовые основы обращения с информацией в информационных системах, включая IoT.

2. Федеральный закон «Об основах обеспечения информационной безопасности Российской Федерации» от 6 февраля 2017 г. №187-ФЗ, определяющий национальные стандарты защиты критической информационной инфраструктуры.

¹ © Брюзгин А. И., 2025.

3. Приказы ФСБ и Минцифры РФ, регламентирующие специфические требования к безопасности объектов критической информационной инфраструктуры, среди которых могут оказаться и системы IoT.

4. ГОСТы и технические регламенты в сфере информационных технологий, направленные на установление стандартов безопасности и защиты информации в сетях, связанных с IoT.

Приведение существующих требований к безопасности IoT в соответствие с международными стандартами является одной из задач государственных органов, что обусловлено динамикой глобальных угроз кибербезопасности.

Анализ угроз в инфраструктуре IoT.

Современные кибератаки на IoT-устройства характеризуются высокой степенью автоматизации, низкой стоимостью реализации и масштабностью воздействия. Основные угрозы включают:

1. Несанкционированный доступ и управление устройствами.

Уязвимости в программном обеспечении IoT-устройств могут использоваться киберпреступниками для получения удаленного доступа, что приводит к нежелательному контролю над системами управления и обработкой конфиденциальных данных.

2. Перехват и подделка данных.

Недостаточная защита каналов передачи информации может привести к атакам типа Man-in-the-Middle (MitM), где злоумышленники меняют данные в процессе их передачи, нарушая целостность и конфиденциальность информации.

3. Доступ к критической инфраструктуре.

Использование IoT-устройств в системах управления промышленными процессами или энергетическими объектами открывает возможность для проведения крупных атак, способных привести к серьезным последствиям, вплоть до аварий и сбоев в работе государственных и корпоративных систем.

4. Атаки на программное обеспечение и прошивки.

Применение несертифицированного или модифицированного программного обеспечения является источником риска внедрения вредоносного кода, что может привести к скрытой эксплуатации устройств для майнинга криптовалют или распространения вредоносных программ.

Совокупность вышеизложенных угроз показывает необходимость выработки и внедрения комплексных мер защиты, направленных как на повышение устойчивости устройств к атакам, так и на оперативное реагирование в случае инцидентов. Для обеспечения безопасности IoT-устройств применяются следующие методы и принципы:

1. Аутентификация и шифрование данных.

Внедрение сильных методов аутентификации пользователей и устройств, а также применение современных алгоритмов шифрования, позволяет снизить риск несанкционированного доступа к данным. Рекомендуется использовать стандарты, подтвержденные ФСБ РФ, для защиты каналов связи.

2. Сегментация сетей.

Разделение сети на логические сегменты позволяет ограничить распространение атак внутри IoT-архитектуры. При этом доступ к критическим компонентам можно контролировать посредством межсетевых экранов (firewalls) и средств VPN-шифрования.

3. Мониторинг и анализ поведения системы.

Использование систем обнаружения и предотвращения нарушений (IDS/IPS) позволяет в режиме реального времени выявлять аномальные действия, что снижает задержки реагирования на попытки проведения кибератак.

4. Регулярное обновление и патчинг.

Своевременное обновление программного обеспечения, исправление выявленных уязвимостей и применение цифровых подписей к прошивкам являются важными мерами, предотвращающими взломы и подмены функционала IoT-устройств.

5. Интеграция стандартов безопасности.

Для создания единой системы защиты необходимо интегрировать национальные и международные стандарты (такие как ISO/IEC 27001) с учетом особенностей IoT-инфраструктуры. Важно, чтобы нормативные правовые акты сочетались с гибкостью в применении технических решений.

Анализ современных угроз и нормативно-правовой среды позволяет сформулировать следующие рекомендации:

6. Разработка специализированных стандартов безопасности для IoT.

На уровне государства следует инициировать создание нормативных документов, учитывающих специфику IoT-технологий, с обязательными требованиями по аппаратной и программной безопасности.

7. Повышение квалификации специалистов.

Обучение профессионалов в области информационной безопасности должно включать современные методики защиты IoT-устройств, а также правовые аспекты кибербезопасности, что позволит быстрее адаптироваться к новым угрозам.

8. Содействие сотрудничеству между государственными органами и частным сектором.

Установление эффективного обмена информацией о кибератаках, проведение совместных учений и разработка единых протоколов реагирования на инциденты помогут повысить общенациональный уровень защиты.

9. Оценка рисков на всех этапах жизненного цикла устройства.

На стадии проектирования, производства и эксплуатации IoT-устройств необходимо проводить оценку рисков, что позволит выявлять потенциальные уязвимости и своевременно принимать меры по их устранению.

10. Внедрение мер мониторинга и аудита.

Создание систем контроля за эксплуатацией IoT-устройств, проведение регулярных аудитов безопасности и тестирование на проникновение должны стать обязательной практикой для всех организаций, использующих данные технологии.

Интернет вещей является важной составляющей современной цифровой экономики, что требует комплексного подхода к обеспечению его безопасности. Ос-

новой эффективной защиты IoT от кибератак является гармонизация нормативно-правовой базы, использование современных технологий аутентификации, шифрования, сегментации сети и мониторинга.

Приведенные рекомендации и практические меры позволяют создать надежную систему защиты, способную противостоять современным киберугрозам, а также создать условия для устойчивого развития цифровой инфраструктуры в России.

Список литературы

1. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 №149-ФЗ// СПС «Консультант Плюс».
2. Федеральный закон «Об основах обеспечения информационной безопасности Российской Федерации» от 06.02.2017 №187-ФЗ // СПС «Консультант Плюс».
3. Технические регламенты и стандарты ФСБ РФ для критической информационной инфраструктуры// СПС «Консультант Плюс».
4. Методические рекомендации Минцифры РФ по защите цифровых коммуникаций// СПС «Консультант Плюс».
5. Международные стандарты ISO/IEC 27001 и ISO/IEC 15408 в контексте применимости к IoT// ISO/IEC 27000 Family – Information Security Management Systems.2018. URL: <https://www.iso.org/isoiec-27001-information-security.html>.
6. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. 2024. № 5. С. 149–155.
7. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. 2023. № 4. С. 88–92.
8. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
9. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
10. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. Москва : Ай Пи Ар Медиа, 2025.
11. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025.

Булатова В. Д.¹,
*курсант института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя*

Научный руководитель:
Михайленко Н. В.,
*доцент кафедры противодействия
 преступлениям в сфере информационно-
 телекоммуникационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат юридических наук, доцент*

ПРАВОВОЕ ЗНАЧЕНИЕ СОТРУДНИЧЕСТВА ОРГАНОВ ВНУТРЕННИХ ДЕЛ СО СМИ В ПРЕДУПРЕЖДЕНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В современную эпоху нарастает острая проблема, связанная с преступлениями в информационно-телекоммуникационной сфере. Эта угроза нависла над всеми странами современного мирового сообщества, которая в силах разрушить политику страны, что приведет уже к более серьезным последствиям, таким как внешняя и внутренняя безопасность страны, законные права и интересы граждан.

Наряду с этим государство старается предпринимать своевременные меры по борьбе с преступлениями в информационно-телекоммуникационной среде, однако развитие таких преступлений набирает «масштабный» характер, злоумышленники подстраиваются под меры, предпринимаемые государством против киберпреступлений, и создают новые способы совершения противоправных деяний с помощью IT сферы.

В свою очередь, в осмыслении общественной опасности от деяний, совершаемых в информационно-телекоммуникационной сфере, играют средства массовой информации. Именно посредством материалов, репортажей, передач, сюжетов, посвященных киберпреступлениям общественность, понимает опасность и тенденцию к постоянному росту таких преступлений.

Каким образом СМИ влияют на профилактику и защиту граждан от таких преступлений?

СМИ в жизни каждого гражданина проявляется в той или иной мере, в качестве новостных сводок на веб-сайтах, группах мессенджеров, помогая людям оценить нарастающую проблему и сложность ее уголовно-правового регулирования. Под СМИ с точки зрения правового характера (понимается тираж или часть тиража отдельного номера периодического печатного издания, отдельный

¹ © Булатова В. Д., 2025.

выпуск телеканала, радиоканала, радиопрограммы, телепрограммы, кинохроникальной программы, тираж или часть тиража, аудио- или видеозаписи программы, отдельный выпуск либо обновление сетевого издания, отдельный выпуск иного средства массовой информации). Функцией СМИ в профилактике преступлений в IT сфере выступает ознакомительная функция, которая знакомит индивида с общественным мнением, динамикой и структурой совершаемых противоправных деяний, а также помогает сформировать прогнозы по их модификации и проанализировав принять соответствующие меры по их пресечению.

Если рассматривать коммуникацию общественности, представителей власти и средств массовой информации, то общественность с психологической точки зрения выбирает представителей СМИ для того, чтобы поделиться своим мнением о происходящем в мире, а сотрудники полиции посредством анализа предоставленной СМИ информацией организует и принимает определенные решения и меры по борьбе с нарастающими проблемами и угрозами.

Заслуживают внимания те публикации и материалы, которые направлены на установление личности преступников, совершающих преступления в информационной сфере, к примеру такого исследования, можно отнести статью из международного журнала «Вестник науки», (авторы Овчинникова Д. Д., Вешкельский А. С.). Данная статья раскрывает личность киберпреступника, особые черты, образ жизни таких людей и уровень образования. Данные лица зачастую имеют высшее образование и особые познания в области информационно-телекоммуникационных технологий. Что в свою очередь дает общественности понимание и особые признаки лиц, совершающих указанные противоправные деяния.

Современный человек использует компьютер не только для общения и развлечений, но и для самореализации и работы, поиска решений в сложных жизненных ситуациях, в том числе преступных схем для получения финансовой или иной выгоды. Эти обстоятельства значительно усложняют работу правоохранительных органов, направленную на исправление и поиск таких правонарушителей, делая профилактику преступлений первоочередной задачей.

Таким образом, предупреждение преступлений, совершаемых с использованием информационных технологий, становится одним из важнейших направлений в деятельности правоохранительных органов, и в данном случае СМИ выступает посредником между органами власти и общественностью. Одним из важных аспектов при таком сотрудничестве выступает работа СМИ по повышению позитивного мнения к органам внутренних дел, которые в основном и несут ответственность по предупреждению, раскрытию и расследованию преступлений, совершаемых с использованием информационных технологий.

СМИ обладают широким механизмом, с помощью которого они влияют на общественное мнение. Публикации, репортажи, статьи, посвященные успешному опыту противодействия преступлениям, связанным с информационно-телекоммуникационными технологиями, а также анализ тактик и методов действий преступников – все это повышает осведомленность граждан и помогает предотвратить новые преступления.

При этом важно не только рассказывать о методах и схемах преступников, но также и рассказывать о мерах, которые смогут помочь защитить себя от их

действий, как следует себя вести в Интернете и как распознавать фишинговые атаки и другие мошеннические схемы. Кроме этого, СМИ также могут эффективно влиять на предотвращение иных массовых беспорядков организуемых с использованием социальных сетей и мессенджеров. В данном случае возникает необходимость в разъяснении юридических последствий в участии подобных не-санкционированных акциях, демонстрации разрушительных последствий таких мероприятий и пропаганда способов мирных решений социальных проблем.

Важно, чтобы эта информация была доступна как для молодежи, которая активно использует цифровые технологии в своей жизни, так и для более взрослого поколения, для которых тяжело проходит адаптация к современным технологиям. Эффективность этой информации будет достигаться путем постоянного анализа и корректировки с учетом изменения ситуации в информационной сфере. Также необходимо использовать разнообразные форматы- от прямых эфиров с участием представителей органов власти до научных статей и статистических данных, чтобы донести информацию до максимального числа людей. Сотрудничество органов внутренних дел с СМИ в этом направлении является необходимым условием для достижения максимальной эффективности профилактики обеспечения безопасности граждан в информационной среде и поддержания общественного порядка.

Таким образом, нарастающая угроза, сопряженная с преступлениями в информационно-телекоммуникационной среде, затрагивает все страны современного мира. Власти государства предпринимает меры по борьбе с этими преступлениями, однако злоумышленники постоянно адаптируются и разрабатывают новые методы. Но посредством осведомления и сбора общественного мнения СМИ выступают связующим звеном между обществом и правоохранительными органами для пресечения и профилактики преступлений в информационной сфере и поддержания общественного порядка.

Список литературы

1. Закон Российской Федерации от 27.12.1991 № 2124-1 (ред. от 23.11.2024) «О средствах массовой информации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_1511/.
2. Овчинникова Д. Д., Вешкельский А. С. Криминологический портрет личности, совершившей преступления в сфере информационных технологий // НИЦ Вестник науки. 2025. № 5 (74). Т 3. С. 506–511.
3. Статданные о преступлениях, совершенных с использованием современных информационно-телекоммуникационных технологий // epp.genproc.gov.ru : [сайт]. URL: https://epp.genproc.gov.ru/web/proc_cfo/mass-media/news/archive?item.
4. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
5. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. Москва : Ай Пи Ар Медиа, 2025.
6. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. Москва : Ай Пи Ар Медиа, 2025.

7. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. 62 с.

8. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2024. С. 35–37.

9. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

10. Михайленко Н. В. Отдельные проблемы цифровизации органов внутренних дел Российской Федерации / Н. В. Михайленко // Актуальные проблемы кибербезопасности в сети Интернет : Сборник научных трудов Всероссийской конференции, Москва, 23 апреля 2020 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2020. С. 102–105.

Буракова А. А.¹,
*курсант института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя*

Научный руководитель:
Токолов А. В.,
*доцент кафедры противодействия
 преступлениям в сфере информационно-
 телекоммуникационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат юридических наук*

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ИСПОЛЬЗУЕМЫЕ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ

В 21 в. ученые достигли огромных успехов во всех сферах жизни общества, будь то образование или правоохранительная деятельность. Время, в которое мы живем можно назвать «информационной эрой». Появилось множество новейшей техники, а также различных специфических технологий. Новшества не обходят стороной и сферы правоохранительной деятельности и обеспечения безопасности граждан. Преступность – исторически изменчивое и высоко адаптивное понятие, означающее, что с развитием технологий развиваются и методы совершения противоправных деяний. Данный факт указывает на то, что преступления, совершаемые в прошлых веках, во многом отличаются от тех, которые возникают в современности. Так, например, в 20-х гг. 20 в. были распространены карманные кражи, в нынешнее же время на их месте стоят информационные преступления. Стоит заметить, что в условиях изменчивости преступности возникает необходимость также менять и технологии, применяемые в расследовании преступлений.

В начале 2000-х гг. в Москве активно начали устанавливаться камеры видеонаблюдения. Основная масса таких камер использовалась в магазинах, торговых центрах и местах, которые требуют особого контроля. В нынешнее время видеонаблюдение находится повсеместно: на парковках, улицах, дворах, в подъездах и любых общественных местах. Современные камеры способны не только записывать видео, но также и распознавать лица, номера машин, движения людей и даже возможное нахождение оружия в руках человека. Данные технологии созданы на базе искусственного интеллекта – компьютерной программы, созданной на основе технологии машинного обучения, которая способна анализировать полученную информацию, а также выдавать ответы на основе передовых алгоритмов. Система инновационных камер видеонаблюдения состоит из множества

¹ © Буракова А. А., 2025.

аппаратов слежения и сервера, на котором установлен искусственный интеллект. Он получает видеоизображения, которые анализирует и сигнализирует о процессах, происходящих на них. К таким технологиям можно отнести систему ANRP (Automatic number plate recognition), данная система способна считывать номерные знаки автомобилей для наложения ответственности за нарушения, совершаемые водителем, а также для упрощения процесса оплаты проезда автотранспортного средства. Программа обеспечивает безопасность дорожного движения, выполняет функции пресечения нарушений и обеспечения неотвратимости ответственности. Так же существуют камеры видеонаблюдения, способные распознать лицо человека и соотнести полученное изображение с изображениями из базы данных. Таким образом возможно производить поиск лиц, находящихся в розыске без привлечения большого объема сил и средств. Помимо определения объекта, камеры на базе искусственного интеллекта способны отслеживать так же его перемещение с помощью контроля видеоизображений с разных устройств. «Умный» сервер может построить маршрут передвижения лица, показав, где находится объект. Данное направление обладает огромным потенциалом, поскольку оно откроет новую веху в раскрытии и расследовании преступлений, а также сделает данный процесс более простым.

Необходимо рассмотреть опыт создания программы для прогнозирования возможных преступлений, как перспективную отрасль развития противодействию преступлениям с помощью информационных технологий. В 2012 г. Департамент полиции Лос-Анджелеса совместно с Калифорнийским университетом разработали систему «PredPol» (predictive policing), способную определить в каком месте и когда предположительно будут совершены какие-либо преступления, такие прогнозы были актуальны в течении 12 часов. Программа работала с помощью сбора и анализа материалов дел и статистики, на основе которых, создавала карту местности, выделяя отдельные участки, на которых, вероятнее всего, произойдет преступление. Данная разработка не стала успешной среди правоохранительных органов, поскольку критиковалась из-за недоработанности, но тем не менее, несмотря на критику, выполняла свою функцию прогнозирования, что является инновационной технологией современности.

Преступность является исторически переменчивым явлением, а также имеет социальную природу, подчеркивая, что вместе с обществом и всеми его сферами развиваются и совершенствуются методы совершения преступлений. Помимо разработок новейших технологий, для удобства жизни человека необходимо так же вводить и инновации, имеющие вспомогательную функцию, для правоохранительной деятельности. Такие технологии во многом увеличат количество раскрытых преступлений, а также помогут в их предотвращении и пресечении.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// Российская газета, № 165, 29.07.2006.

2. Федоров М. Н. Преступления, совершаемые с помощью глобальной информационной сети Интернет.
3. Батурин Ю. М. Проблемы компьютерного права / Батурин Ю.М. М.: Юрид. лит., 1991.
4. Беспалова Е. В., Широков В. А. Киберпреступность: история уголовно-правового противодействия // Информационное право. М.: Юрист, 2006, № 4 (7).
5. Дворецкий М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография / М. Ю. Дворецкий.
6. Голубев В. А. Компьютерная преступность: состояние, угрозы и прогнозы // Компьютерная преступность и кибертерроризм. Сборник научных работ: вып. № 2. Запорожье: Центр исследования компьютерной преступности, 2004.
7. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.
8. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
9. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.
10. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
11. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
12. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
13. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

Варванская А. В.¹,
студент 4 курса, факультет права
НИУ «Высшая школа экономики», г. Москва

Красовская М. А.²,
студент 4 курса, факультет права
НИУ «Высшая школа экономики», г. Москва

Научный руководитель:
Пушкарев В. В.,
доцент департамента уголовного права,
процесса и криминалистики
НИУ «Высшая школа экономики»,
кандидат юридических наук, доцент

ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПО ДЕЛАМ, СВЯЗАННЫМ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙНА: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

В эпоху глобальной информатизации и цифровизации общество является свидетелем увеличения количества преступлений, совершаемых в киберпространстве: так, по данным, обнародованным МВД России, в 2024 г. лишь в нашей стране было зафиксировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий [1]. Примечательно, что по сравнению с прошлым годом число преступлений в данной сфере выросло в процентном соотношении на 13,1 %, и имеются все основания полагать, что в обозримом будущем тенденция по их стремительному росту будет носить еще более ярко-выраженный характер. Одним из инструментов в руках преступников является технология блокчейн, в частности, основанная на ней криптовалюта, характеризующаяся трудностью отслеживания и отсутствием централизованного контроля. Более того, криптопреступники предпринимают попытки использования разнообразных методов по анонимизации транзакций, что бросает серьезный вызов для имеющихся механизмов профилактики правонарушений и побуждает искать инновационные подходы к расследованию и доказыванию, включая блокчейн-аналитику для повышения эффективности в борьбе с киберпреступностью. Использование инструментов анализа блокчейна, таких как Chainalysis, Elliptic, MistTrack и прочих, позволяет сочетать технологическую прозрачность при помощи аналитики данных. Несмотря на растущий интерес к блокчейну, темы, связанные с его использованием в качестве доказательств, исследованы лишь частично. Не существует на данный момент также общепринятых стандартов для оценки таких доказательств, что повышает значимость темы настоящего исследования. Имеются также глобальные различия в

¹ © Варванская А. В., 2025.

² © Красовская М. А., 2025.

процессуальном законодательстве разных стран в области криптовалюты. Сравнительный анализ этих подходов, который будет проведен в рамках работы, позволяет выявить наиболее эффективные решения и перспективы для глобального сотрудничества. Важно также рассмотреть потенциал, который включает в себе блокчейн как инструмент доказывания. Неизменяемость данных делает его идеальным источником раскрытия финансовых преступлений, мошенничества, отмывания денег, однако данная концепция еще не внедрена в широкую практику, что было бы крайне актуально в эпоху цифровизации, когда государственно-правовые системы сталкиваются с неминуемой необходимостью адаптироваться к новым реалиям.

Говоря о таком феномене, как криптопреступность, следует иметь в виду, что под ним в рамках настоящего исследования в самом общем смысле будет пониматься совокупность широкого круга общественно опасных деяний, для совершения которых в определенных формах и объеме задействуются блокчейн-технологии. В научной тематической литературе также выделяются подходы к пониманию криптопреступности: например, ряд авторов справедливо нарекает ее в качестве формы киберпреступности как явления более широкого. Наиболее популярным аргументом в защиту данной позиции является тот факт, что криптовалюты, такие как Bitcoin и Monero, становятся инновационным инструментом для совершения классических преступлений в киберпространстве (фишинг, отмывание денег, вымогательство), но не порождают новых: благодаря мнимой (о чем пойдет речь далее) анонимности, а также децентрализации цифровых валют происходит лишь оптимизация уже существующих методов, что отнюдь не изменяет исконную природу самого преступления [2]. Происходит лишь адаптация криптовалюты для старых, уже известных целей, вместе с внедрением инновационных технологий. Согласно еще одному доктринальному воззрению, криптопреступность частично связана и с экономической преступностью, так как посягает именно на общественные отношения, имеющие тесную связь с экономической средой, и влияет на финансовую деятельность граждан, организаций и государства [3]. Следует поддержать и этот аргумент, поскольку преступления в криптосфере характеризуются системой незаконных финансовых операций, где криптовалюта выступает в качестве инструмента для обхода регуляторных механизмов, открывая злоумышленникам простор для совершения ряда противозаконных действий.

Так, плавно перейдем к рассмотрению видов криптовалютных преступлений, которые охватывают крайне широкий перечень. В научных исследованиях условно выделяются три основных направления развития киберпреступности, такие как: легализация (отмывание) средств, полученных преступным путем, посредством криптовалюты; незаконный оборот запрещенных или изъятых из оборота предметов (приобретение, сбыт наркотических средств, психотропных веществ, порнографии и др.); преступления против собственности, в том числе хищение криптовалюты [4]. Среди конкретных видов преступлений, согласно статистическим данным за прошедший год, наиболее частыми являются материалы о жестоком обращении с детьми; создание, использование и распростране-

ние вредоносных компьютерных программ; финансирование терроризма и незаконная деятельность (мошенничество) [5]. Следует также отметить, что в зависимости от направления и вида совершаемого преступления злоумышленниками используются различные методы и схемы. Например, весьма распространенным инструментом для легализации средств, полученных преступным путем, является использование так называемых «миксеров» – сервисов, принцип работы которых заключается в принятии криптовалюты от множества пользователей, смешивании ее в общем пуле, а затем распределении средств на новые адреса, что разрывает связь между исходными и конечными транзакциями, повышая анонимность последних. В сегменте преступлений против собственности среди инструментов наиболее распространены фишинговые атаки, когда мошенники создают поддельные сайты или электронные кошельки, а также взломы криптобирж, атаки программ-вымогателей. Отдельно стоит поговорить про широкую популярность использования ICO – проектов для преступных целей. ICO, или Initial Coin Offering представляет форму привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной генерацией. Тем не менее, отсутствие должного регулирования и контроля со стороны государственных органов привело к организации мошенниками компаний, направленных на сбор денег без намерения выполнить обязательства перед инвесторами. При рассмотрении преступлений, связанных с незаконным оборотом запрещенных или изъятых из оборота предметов, в частности, наркотических средств, можно выявить ряд свойств криптовалюты, благодаря которым последняя интегрируется в противоправную деятельность. К таковым относится децентрализация, исключающая необходимость посредников, таких как банки, что упрощает транзакции без проверки легитимности операций, а также высокая скорость транзакций и низкие комиссии, что позволяет преступникам быстро и дешево перемещать крупные суммы между кошельками, минимизируя время для их обнаружения. Отдельно следует затронуть и такое свойство, как анонимность, степень которой варьируется от вида криптовалюты. Так, например, транзакции биткоина полностью прозрачны: они не содержат прямых данных о личностях пользователей – вместо этого используются криптографические адреса, однако все транзакции с ними публично записываются в блокчейн, остаются там навсегда и хранятся в открытом доступе. Описанную выше историю платежей можно отследить в случае, если адрес кошелька каким-либо образом связан с личностью (например, при прохождении верификации на криптобирже). В связи с этим научная литература нарекает биткоин свойством «псевдоанонимности» – возможности раскрытия личности. Совершенно иной случай – такой вид криптовалюты, как Monero. Ее отличает повышенная гарантия анонимности «по умолчанию» за счет кольцевых подписей, подразумевающих подпись транзакции группой пользователей, что исключает возможность определить действительного отправителя; скрытых адресов, означающих процесс генерации для каждой транзакции одноразового адреса получателя, скрывающего его реальный кошелек; а также конфиденциальности самой транзакции – шифруется также сумма. Второй упомянутый вид цифровой валюты по очевидным причинам находит наибольший отклик среди преступников.

Между тем существуют и другие методы повышения анонимности: к примеру, уже рассмотренные в рамках исследования «миксеры». Все это создает непосредственную угрозу для обеспечения безопасности: методы и схемы, используемые преступниками в криптосфере развиваются и совершенствуются. Тем не менее в состоянии непрерывной эволюции находятся также и механизмы противодействия криптопреступности, которые будут более подробно рассмотрены ниже.

На сегодняшний день существует достаточное количество специализированных коммерческих сервисов, осуществляющих функции по анализу, идентификации и деанонимизации подозрительных транзакций. К таковым относится, например, компания Chainalysis – на ее примере для целей настоящего исследования будут рассмотрены возможности вклада подобных платформ в доказывание и расследование преступлений в криптосфере. Итак, Chainalysis, основанная в 2014 г., сейчас выросла до одной из ключевых компаний в области анализа блокчейна: ее технологии помогают обеспечивать прозрачность и безопасность в криптовалютной индустрии, способствуя массовому принятию и регулированию последней. Поэтому, неудивительно, что услугами Chainalysis активно пользуются государственные органы, биржи, финансовые учреждения, страховые компании и компании по кибербезопасности в более чем 70 странах [6]. Рассматриваемый сервис осуществляет свою деятельность, руководствуясь рядом основополагающих принципов. Начать следует с основного, а именно стремления к повышению прозрачности: связано это с тем, что основным препятствием на пути к интегрированию криптоиндустрии в традиционную финансовую инфраструктуру является отсутствие доверия между правоохранительными органами, регулирующими органами и криптовалютными компаниями. Chainalysis же видит решение этой проблемы в разработке более четких правил, стандартизации методов аудита и применении мощного контроля соответствия – все для того, чтобы криптовалюта продолжала расти [7]. Следуя поставленной миссии, Chainalysis разделяет всю свою деятельность на две крупные категории: продукты и решения. К продуктам относятся инструменты, позволяющие обеспечить безопасность индустрии блокчейн. Одним из наиболее распространенных является Reactor – программное обеспечение, позволяющее пользователям отслеживать движение криптовалюты, выявлять подозрительные активности, устанавливать связи между различными анонимными адресами кошельков и, в итоге, связывать их с реальными лицами или организациями, устанавливая тем самым личность подозреваемых. Reactor, будучи мощным инструментом анализа транзакций и придания им прозрачности и отчетности, необходимых, в свою очередь, для обеспечения законности, поддерживает анализ транзакций в блокчейнах Bitcoin, Ethereum, Litecoin и других популярных криптовалют, а также работает и с приватными монетами, такими как Monero (XMR). О подобном многообещающем потенциале продукта Chainalysis может свидетельствовать относительно недавняя утечка видео компании: его содержание сводится к методам отслеживания Monero, позиционирующей себя как приватную и полностью конфиденциальную криптовалюту [8]. Ко второй категории, предлагаемой Chainalysis, относятся услуги по решению проблем в области нарушения кибербезопасности: речь

идет про разработанные компанией методики по обнаружению и расследованию криптопреступлений, а также стандарты, содержащие как местные, так и международные правила, и нормы, которые различные фирмы и платформы могут внедрить в рабочий процесс для правильного управления рисками при построении стратегий, предложений и партнерств, основанных на криптовалютах. Среди явных признаков деятельности Chainalysis также следует упомянуть балансирование компании между деанонимизацией транзакций в преступных целях и обеспечением приватности для законопослушных пользователей криптовалюты. Наконец, заключительным принципом деятельности Chainalysis, очевидно вытекающим из описанного нами ранее стремления к прозрачности, является призыв компании к сотрудничеству организаций, работающих на крипторынке (например, криптобиржам) с целью выполнения требований регуляторов; финансовым организациям, заинтересованным в соблюдении антиотмывочного законодательства; государственным структурам (налоговым службам, подразделениям финансовой разведки, правоохранительным структурам) [9]. Достичь же этого сотрудничества, как уже было выяснено, поможет повышение доверия к криптовалюте, как к видимой в обозримом будущем составляющей мировой финансовой отрасли.

Еще одним аналитическим сервисом является Elliptic – компания, использующая передовые технологии, включая методы анализа данных и машинного обучения, для отслеживания подозрительных транзакций, в том числе прошедших через «миксеры». Ранее в рамках настоящего исследования, данная тема уже неоднократно затрагивалась, однако таким образом выражается стремление обратить внимание на ее животрепещущий характер: криптомиксеры значительно усложняют отслеживание транзакций, в связи с чем их использование несет большое количество рисков – от репутационных до правовых. Так, например, в США использование миксеров может рассматриваться в качестве признака незаконной деятельности: об этом свидетельствует предложение департамента по борьбе с финансовыми преступлениями Министерства финансов классифицировать криптомиксеры как «основной инструмент для отмывания денег». Сегодня в Соединенных Штатах против миксеров, таких как Tornado Cash, вводятся санкции, а биткоин-платформы предупреждают пользователей о бессрочной блокировке за использование данных инструментов. И все же, на данный момент прямого запрета на миксеры во многих юрисдикциях все еще не наблюдается, что является следствием недооценивания регуляторами опасности, которую те в себе несут. При тех негативных последствиях, которые подразумевает использование миксеров, потенциальные выгоды от повышения анонимности транзакций за их счет кажутся неоправданными. Возвращаясь к Elliptic, рассмотрим подходы, используемые компанией для распутывания, транзакция, прошедших через процесс «микширования»: к ним можно отнести кластеризацию адресов, поиск алгоритмами характерных паттернов транзакций, установление связи между транзакциями за счет времени поступления и вывода средств и прочее. На счету у компании несколько громких дел, закончившихся успешным отслеживанием движения украденных средств (расследование взлома криптобиржи KuCoin в

2020 г.) и выявлением связей между криптокошельками (кибератака на Colonial Pipeline в 2021 г.) после применения вышеперечисленных алгоритмов.

Так, наконец, перейдем к главному тезису, выдвигаемому в настоящем исследовании: его содержание сводится к перспективности такого метода доказывания в расследование преступлений, связанных с криптовалютой, как внедрение разработок частных компаний. Связано это со многими аспектами, среди которых отметим, например, недостаток осведомленности государственных структур об особенностях функционирования блокчейн-технологий, на которых и построена криптовалюта, с этим связана и проблема отсутствия доступа к передовым инструментам по анализу блокчейн-транзакций. Частные же фирмы, как правило, специализируются в данной области, располагая высоко компетентными экспертами, постоянно следящими за новыми тенденциями и методами, используемыми преступниками, а также инновационными технологиями, включая графовый анализ, машинное обучение и большие данные для отслеживания транзакций. Кроме того, частные фирмы, в отличие от неповоротливых государственных структур, в меньшей степени сталкиваются с юридическими и бюрократическими барьерами, которые замедляют процесс расследования – это помогает первым действовать более гибко и оперативно, что особенно важно в случаях, требующих быстрого реагирования. Также немаловажно, что криптопреступления зачастую носят трансграничный характер, что затрудняет расследование для государственных органов – частные аналитические компании же преодолевают данный юридический барьер с куда меньшей затратностью, сотрудничая с правоохранительными органами разных стран (как в случае с Chainalysis), что повышает эффективность раскрытия преступлений.

Таким образом, частные фирмы заключают в себе действительно ценный ресурс для института доказывания в уголовном процессуальном праве. Например, визуализация цепочек транзакций, показывающая движение средств между кошельками, может помочь правоохранительным органам в выявлении подозрительных паттернов, таких как использование миксеров. Производимые аналитическими компаниями детализированные отчеты о движении средств, содержащие информацию о транзакциях, временных метках, суммах и адресах кошельков, могут также являться доказательствами, устанавливающими связь между кошельками и реальными лицами. Сама по себе информация о времени и суммах транзакций может установить временную последовательность событий и выявить подозрительную активность. Вместе с тем допустимо говорить о процессе внедрения минимального стандарта ответственности для аналитических компаний при сотрудничестве с государственными органами в расследовании криптопреступлений. Полагаем целесообразным предусмотреть обязанность по соблюдению конфиденциальности данных и защиты их от несанкционированного доступа, а также обеспечению высокой точности и достоверности предоставляемых результатов работы – в случае же выявления ошибок справедливо говорить об их исправлении и компенсации ущерба при наступлении негативных последствий.

Процессуальное законодательство в области криптовалюты демонстрирует значительные различия между странами, затрагивая вопросы допустимости доказательств, взаимодействия с технологическими платформами и стандартов расследования. Для целей нашего исследования считается уместным проведение краткого сравнительно-правового анализа.

Начнем непосредственно с отечественного законодательства, которое сохраняет процессуальные пробелы: УПК РФ не предусматривает специальных норм для блокчейн-доказательств, что приводит к необходимости назначать комплексные технические экспертизы – все это значительно усложняет эффективность раскрытия преступлений. В США ситуация варьируется от штата к штату: в Калифорнии, например, суды допускают данные блокчейн-аналитики (например, отчеты Chainalysis) как доказательства без обязательной сертификации инструментов. В Сингапуре, в рамках «Закона о платежных услугах», криптокомпаниям обязаны вести учет, а также хранить информацию о клиентах и транзакциях в течение пяти лет [10], а суды в делах (например, CLM v. CLN, 2022) признают отчеты блокчейн-аналитиков как допустимые доказательства. В Швейцарии ситуация аналогична: записи в блокчейне признаются в качестве электронных доказательств при условии их соответствия требованиям достоверности, что подтверждается, например, через деятельность аудиторов. Что касается уголовных расследований, то и здесь криптотранзакции отслеживаются с помощью инструментов вроде Chainalysis, также правоохранительные органы сотрудничают с биржами в рамках закона «О противодействии отмыванию денег» (AMLA) [11].

Таким образом, сравнительно-правовой анализ позволяет судить о значительных различиях, обусловленных технологическими, правовыми и культурными особенностями юрисдикций различных стран при подходе к процессуальному регулированию инструментов блокчейна как средства доказывания в криптопреступлениях. Отметим, что успешное расследование во многом зависит от международной кооперации, однако без унификации процессуальных норм и создания глобальных механизмов доверия к блокчейн-доказательствам, эффективное правоприменение так и останется фрагментированным.

Для полного понимания и погружения в проблематику обозреваемой темы, считается необходимым обратиться к практике применения разработок частных фирм для обеспечения публичного интереса при расследовании и доказывании разного рода преступных деяний в криптовалютной сфере.

Так, стоит обратить внимание на дело об интернет-магазине «Silk Road», располагавшемся в сети «Tor». Данный «маркетплейс» имел функционал, позволяющий пользователям приобретать и продавать различные товары, большинство из которых принято считать запрещенными для распространения. Описываемое расследование богато множеством дискуссионных аспектов и интереснейших способов доказывания вины владельца «Silk Road» – Росса Уильяма Ульбрихта, к чему обратимся чуть позже в нашей статье. В рамках конкретной части работы, релевантнее обратить внимание на один из методов поиска улик, против упомянутого подозреваемого. Так, агенты Службы внутренних доходов (IRS-CI) Соединенных Штатов Америки (далее – США) использовали разработку компании

Chainalysis – Reactor, что в итоге принесло свои плоды и позволило им обнаружить 54 ранее необнаруженных транзакций биткоинов, представляющих собой доходы от незаконной деятельности интернет-магазина «Silk Road». Это программное обеспечение помогает расследовать всевозможные взаимодействия лиц с криптовалютой посредством связи крипто кошельков или транзакций блокчейна с действительными объектами. То есть, проще говоря, Chainalysis обладает большой базой данных, в которой хранятся ранее проанализированные профили бирж, адреса кошельков криптовалют.

В несколько схожем расследовании против аналогичного интернет-магазина «AlphaBay» следователи также обращались за помощью к Chainalysis, а именно к одному из его владельцев компании - Джонатану Левину, который раскрывает путь криптовалютных транзакций второго «маркетплейса» под названием «Hansa», уходящий на территорию Литвы, где, как выяснится, находится центр управления данными. Такое открытие позволит европейским правоохранительным органам взять под контроль теневой рынок распространения запрещенных веществ, что сыграет на руку американским следователям в поимке мигрирующих с «AlphaBay» продавцов упомянутой ранее продукции.

Также Reactor был использован государственными органами США для анализа транзакций блокчейна спонсоров и пользователей сайта «Welcome to Video», на котором размещались порнографические материалы с участием несовершеннолетних лиц. Таким образом, это стало как частью доказательств вины оператора сайта, так и способом облегченного поиска причастных к функционированию сервиса «Welcome to Video». Поскольку пользовательская сетка данного сайта распространилась по всему земному шару, правоохранительные органы десятков стран получили необходимые инструкции по использованию платформы «Chainalysis» и поимке необходимых преступников.

Взглянув на приведенную краткую сводку примеров применения разработок частной фирмы, предназначенных для повышения эффективности расследований в области криптовалютного оборота, можно помыслить, что благодаря подобному высокотехнологичному инструментарию проблема криптопреступности не стоит так остро, как иные формы киберпреступлений, однако, на наш взгляд, это не является правдой, что станет более очевидным в следующих разделах настоящего исследования.

Далее считаем важным детально рассмотреть методы расследования преступлений, связанных с криптовалютой, что позволит определить наиболее важные аспекты доказывания вины подозреваемых, а также выделить эффективные способы расследования.

Прежде всего, необходимо выделить следующие дефиниции: доказывание - познавательная деятельность, осуществляемая посредством собирания, проверки и оценки доказательств на досудебных стадиях и направленная на выявление и изобличение лица, совершившего преступление [12]. По сути, данный этап есть фундаментальный элемент уголовного процесса, определяя сущностную ценность уголовного правоприменения. Многие исследователи, в том числе и Н. В. Шепель, полагают, что релевантнее применять индивидуальный подход в рас-

следовании и доказывании различных видов криптовалютных преступлений, которые и будут рассмотрены далее. Так, расследования преступлений в области майнинга, то есть генерации новых криптовалют посредством компьютерных технологий, предполагает осуществление осмотра помещения, где может быть обнаружена техника и кабели для майнинга без необходимых приборов учета. Также есть смысл в поиске информации от сбытовых организаций о резком увеличении потребления электроэнергии на обслуживаемых ими территориях.

Далее особенно популярным видом преступлений в рассматриваемой среде являются махинации, связанные с обменом криптовалют. В данном случае могут признать доказательствами такие носители информации, как онлайн переписки, записи с камер видеонаблюдения, снимки экрана, выписки банковского счета и тому подобное.

Не менее распространенными считаются кражи криптовалют. Методами расследования и доказывания могут стать изучение снимков экрана с необходимой информацией, а также извлечение подробностей произошедшего у потерпевшей стороны. Подобные же действия следователей возможны при расследовании мошенничества, что часто можно встретить в инвестиционных проектах [13]. Немаловажным кажется и уделение внимания таким составам, в которых криптовалюта выступает в роли средства совершения преступления. Технологичность рассматриваемой ситуации создает необходимость исследования цифрового следа подозреваемых вместе с их непосредственными гаджетами, где может храниться ценная информация. Отметим, что во всех приведенных выше случаях правоохранительные органы стараются тесно сотрудничать с Федеральной службой по финансовому мониторингу (далее – Росфинмониторингом), из-за чего возможна более детальная проверка всех интересующих финансовых активов.

Все же, на наш взгляд, приведенные способы расследования криптопреступлений могут показаться чрезмерно хрестоматийными для такой передовой технологии, как цифровая валюта. Такое обстоятельство не может остаться без нашего внимания, поэтому предлагаем поискать дополнительные методы доказывания через призму функционала самой криптовалюты. Так, нетрудно догадаться, что криптовалюта не обладает абсолютной анонимностью, о чем сообщал в своем письме создатель Биткойна (Bitcoin) – Сатоши Накамото [14]. Прозрачность транзакций позволяет применять алгоритмы глубокого анализа данных, которые, в свою очередь, способствуют раскрытию схем и лиц, задействованных при взаимодействии с криптовалютой. Более того, следует учитывать, что зачастую криптовалюта приобретается и обменивается на специализированных рынках, сотрудничество с которыми даст доступ правоохранительным органам к разного рода персональным данным преступников. Также для указанных выше манипуляций с криптовалютой пользователь должен располагать электронным кошельком, открытие которого возможно при помощи криптоключа, его потеря же чревата утратой всех монет. Знание подобных тонкостей способствует обнаружению необходимых крипто-операций. Исследователи, А. Б. Судницын и В. В. Молоков, в частности, обращают особое внимание на крайней важности установления всех деталей перемещения криптовалюты. Так, предлагается во время

допросов делать акцент именно на вопросах, связанных с финансовыми операциями [15]. Если же первостепенной целью перед следователями стоит деанонимизация лица, распоряжавшегося криптовалютой, предлагается, помимо прочего, применять инструменты интернет-разведки. Данный метод подразумевает поиск ценной информации из различных источников, как это имело место в уже упомянутом расследовании против Silk Road.

Изучив приведенную выше информацию, целесообразно сделать вывод о том, что современное следствие обладает некоторой системностью относительно даже сверхновых областей для преступлений, однако присутствует и значительное поле для усовершенствований. Например, немногие авторы впринципе выделяют в качестве способа расследования и доказывания возможность обращения в частную профессиональную фирму, а часть исследователей, которые все же увидели в таком варианте перспективность, не стали особенно расписывать его преимущества, что видится серьезным заблуждением. Данную догадку подтверждают частые упоминания «непреодолимой на настоящий момент технологии шифрования данных», которая заключается в использовании разного рода миксеров, то есть программ, предназначенных для отмыwania криптосредств (Peel chain). В таком утверждении, кажется, кроется значительная доля пренебрежения изучением тех самых профессионализированных компаний, которые уже научились не только распутывать клубки финансовых операций, созданных миксерами, как это успешно получается у MistTrack, но и отслеживать одни из самых анонимных криптовалют, на что намекнула компания Chainalysis.

Следующее, в своей работе А. Б. Судницын и В. В. Молоков упомянули автороведческий анализ, благодаря которому в результате интернет-разведки можно будет установить автора какого-либо текста в онлайн среде. Как некое дополнение ко всему прочему, упомянуть подобный метод расследования и доказывания возможно, однако в труде указанных авторов ему выделено больше внимания, чем объяснению эффективности привлечения частных специализированных организаций. Более того, в эпоху стремительного развития цифровизации тяжело найти человека, который смог бы разобраться в функционале криптовалют, но одновременно не способен скрыть авторские особенности в оставляемых им на просторах сети Интернет текстах, особенно учитывая наличие показательного опыта последствий небрежности у Р. У. Ульбрихта (Ross William Ulbricht).

Обобщая вышесказанное, отметим, что активное развитие следственных мероприятий все же уступает скорости эволюции технологий. К последнему проще адаптируется частный сектор, когда как правоохранительные органы в современном мире всегда идут в совокупности с тяжеловесной машиной государственности, не способной в сжатые сроки изменить свой цифровой быт. Именно поэтому, на наш взгляд, очень важно изучать и стараться применять в расследования криптопреступлений опыт и разработки частных компаний.

Согласно воззрениям авторов настоящего исследования, международное сотрудничество в сфере расследования и доказывания криптопреступлений является основополагающим фактором успешного раскрытия дела, так как криптовалюта не обязана иметь привязку к какой-либо государственной территории для

нормального функционирования, из-за чего подобные отношения часто отягощаются иностранным элементом, игнорирование которого в лучшем случае приведет к увеличению длительности расследования дела. Для более яркой иллюстрации такого тезиса обратимся к наглядным примерам, мнениям экспертов и другим информационным источникам.

Так, если представлять криптовалюту именно как средство для совершения преступления, то на ум сразу приходят ассоциации с незаконным оборотом наркотических и психотропных веществ. Подобное умозаключение небезосновательно, так как с развитием технологий весь черный рынок перекочевал на просторы многослойного Интернета, заняв наиболее зашифрованные и анонимные уровни сети. Несмотря на указанное обстоятельство, некоторые следователи полагают, что даже в случаях очевидно сопряженных с иностранным элементом не всегда есть место международному сотрудничеству, так как нет единого понимания правового статуса криптовалюты, что подтверждается правоприменительной практикой, согласно которой преступления о легализации при помощи криптовалюты средств, полученных с продажи наркотиков, не получают специальной квалификации. Однако А. Г. Волеводз считает, что это не совсем точное мышлеполагание, так как судебная практика все же имеет примеры применения такой квалификации, а также юридическая доктрина располагает некоторыми вариантами разрешения проблемы определения статуса криптовалюты. Более того, по мнению исследователя, популяризация таких воззрений только отдаляет нас от возможности полноценного объединения усилий против криптовалютных злодеяний. Также А. Г. Волеводз отмечает: «существующая международно-правовая база не препятствует международному сотрудничеству в сфере уголовного судопроизводства по рассматриваемой категории дел», то есть даже в условиях отсутствия четко сформулированных норм о криптовалюте государства находят выходы к успешному сотрудничеству между собой [16]. Важно в этой связи отметить принятие Директивы 2018/843 Европейского парламента и Совета об изменении Директивы ЕС 2015/849 о предотвращении использования финансовой системы в целях отмыwania денег или финансирования терроризма и изменении Директив 2009/138/ЕС и 2013/36/ЕС [17]. Подобные документы имеют своей целью объединить государства-участницы Европейского союза для проведения более эффективных расследований криптопреступлений.

Одной из основных проблем затруднительной работы российских правоохранительных органов относительно расследования дел с рассматриваемым составом, как полагает упомянутый автор, является пренебрежение следователями возможности изучения доказательств, находящихся за рубежом, что «противоречит интересам полного раскрытия и расследования таких преступлений, выявления всего круга лиц, виновных в их совершении, предупреждения таких преступлений как на внутригосударственном, так и международном уровнях» [18].

Сложно не согласиться с позицией А. Г. Волеводза, однако необходимо заметить несколько важных особенностей. Во-первых, в существующих реалиях российским следователям может быть сложнее получать необходимые ответы на их запросы некоторым странам. К сожалению, на раскрываемость преступлений с

иностранным элементом огромное влияние оказывает геополитическая обстановка. Во-вторых, есть большие сомнения относительно функционирования международного права. Есть достаточно популярная позиция относительно принимаемых межгосударственных соглашений, согласно которой такие документы создаются «для своих, а не для нас», имея в виду «фиктивность» многих постулатов, выдвигаемых институтами международного права. В связи с таким пониманием появляется основание для сомнений в полноценном воплощении норм, закрепленных в упомянутых директивах. Такие аспекты важно учитывать для того, чтобы логически и идейно укреплять позицию в поддержку установления крепких межгосударственных связей, что безусловно видится для авторов настоящего исследования ценным и основополагающим элементом расследования криптопреступлений.

Размышляя о ценности анонимности и тем более самостоятельности в контексте расследования и доказывания криптопреступлений, необходимо в первую очередь ответить для себя на вопрос о влиянии на наши жизни института государственности. Именно степень погружения личности в государственную мораль определяет и ее отношение к таким понятиям, как анонимность и самостоятельность в целом.

Так, любое государство, рассматривая его метафорически, как некое живое существо, стремится к выживанию, что и заставляет власть имущих диктовать народу ту мораль, которая будет подпитывать жизненную энергию государства. Такое суждение заставляет сопоставить наличие у народа высокой ценности своей анонимности, самостоятельности с выгодой для государственности от распространения подобных прав. В результате несложных размышлений, приходим к выводу, что этатистское устройство общества вероятнее не примет такие ценности, потому что они по естеству своему противоречат основному желанию государства – выжить. Если народ внезапно обретет высокий уровень правопонимания и найдет смысл в поддержании личной анонимности и самостоятельности, государству будет сильно сложнее поддерживать свою гегемонию и продолжать вскармливать веру граждан в необходимость своего существования.

Говоря о самостоятельности и анонимности без учета государственной составляющей, необходимо отметить, что анонимность касательно функциональности криптовалюты относительна, однако она все же обладает меньшей контролируемостью со стороны властей, чем и заслужила повышенное внимание со стороны преступников. В этом смысле кажется стремление к анонимности и самостоятельности достаточно пагубным занятием. Чтобы не заблуждаться в своих домыслах, нужно учитывать также и следующий аспект: зачастую любая система, имеющая в своем фундаменте такие понятия, как анонимность и самостоятельность, обладают высокой степенью саморегуляции, из-за чего сама система способна вырабатывать специализированные институты, способствующие улучшению состояния общего. Так, до недавнего времени монета Monero (XMR) считалась одной из самых анонимных среди своих конкурентов, так как позволяла скрыть источник и получателя средств. Однако, упомянутая в ранней части

работы компания, Chainalysis сумела значительно понизить конфиденциальность Монеро, что позволило отслеживать местоположение взаимодействовавших с «вредоносным» узлом кошельков.

Более того, системы, обладающие в своей основе ценностью самостоятельности, анонимности, а в последствии и саморегуляции, в принципе расположены к отмеченному выше высокому уровню правосознания, из-за чего участники подобных объединений постепенно способны самостоятельно определять, исправлять и предотвращать менее благополучные проявления общего функционирования.

Конечно, есть место и для утверждений об утопичности вышеописанных идей, однако они здесь указаны лишь для обогащения критической мысли и более глубинного осмысления проблематики. Ведь так или иначе блокчейн-анализ, международное сотрудничество, регулирование и обучение специалистов – все это способствует повышению уровня борьбы с киберпреступностью. В будущем можно ожидать дальнейшего развития этих мер, что сделает анонимность и самостоятельность менее привлекательными для преступников, сохраняя при этом их ценность для законопослушных пользователей.

Список литературы

1. Число киберпреступлений в России // TADVISER URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D0%B9_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8 (дата обращения: 08.02.2025).
2. The Role of Cryptocurrency in Cybercrime: Tracking Transactions and Uncovering Networks // ResearchGate URL: https://www.researchgate.net/publication/382176440_The_Role_of_Cryptocurrency_in_Cybercrime_Tracking_Transactions_and_Uncovering_Networks (дата обращения: 08.02.2025).
3. Маздогова З. З., Шигалугова М. Х. Понятие киберпреступности в системе киберпреступлений // Журнал прикладных исследований. 2023. №7. URL: <https://cyberleninka.ru/article/n/ponyatie-kriptoprestupnosti-v-sisteme-kiberprestupleniy> (дата обращения: 05.02.2025).
4. Сидоренко Э. Л. Киберпреступность как новое криминологическое явление // Общество и право. 2018. № 2 (64). URL: <https://cyberleninka.ru/article/n/kriptoprestupnost-kak-novoe-kriminologicheskoe-yavlenie> (дата обращения: 05.02.2025).
5. Основные направления криптовалютных преступлений в 2024 году // AML Crypto.io URL: <https://amlcrypto.io/ru/blog/osnovnye-napravleniya-kriptoprestuplenij#2> (дата обращения: 08.02.2025).
6. Official website of the Chainalysis company. URL: <https://www.chainalysis.com/chainalysis-kyt/> (дата обращения: 12.02.2025).

7. Что такое Chainalysis? // Gate Learn URL: <https://www.gate.io/ru/learn/articles/what-is-chainalysis/869> (дата обращения: 12.02.2025).
8. Chainalysis отслеживает транзакции Monero? // Bitget URL: <https://www.bitget.com/ru/news/detail/12560604199193> (дата обращения: 12.02.2025).
9. Дурандина А. П. Государственная система мониторинга операций в криптовалюте // Инновации и инвестиции. 2021. № 2. С. 110–113.
10. Регулирование криптоактивов в Сингапуре // YB Case URL: <https://ybcase.com/fintech/regulirovanie-kriptoaktivov-v-singapore> (дата обращения: 08.02.2025).
11. Federal Act on Combating Money Laundering and Terrorist Financing // Fedlex URL: https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en (дата обращения: 08.02.2025).
12. Шепель Н. В. Некоторые особенности доказывания при расследовании преступлений, связанных с использованием криптовалют и других виртуальных активов // Общество, право, государственность: ретроспектива и перспектива. 2022. № 3 (11). – С. 94. URL: <https://cyberleninka.ru/article/n/nekotorye-osobennosti-dokazyvaniya-pri-rassledovanii-prestupleniy-svyazannyh-s-ispolzovaniem-kriptovalyut-i-drugih-virtualnyh> (дата обращения: 29.11.2024).
13. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System // Bitcoin P2P e-cash paper. – 2008.
14. Судницын А. Б., Молоков В. В. Отдельные возможности получения и использования сведений об операциях с криптовалютой при раскрытии и расследовании преступлений // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). – С. 218. URL: <https://cyberleninka.ru/article/n/otdelnye-vozmozhnosti-polucheniya-i-ispolzovaniya-svedeniy-ob-operatsiyah-s-kriptovalyutoy-pri-raskrytii-i-rassledovanii-prestupleniy> (дата обращения: 27.11.2024).
15. Волеводз А. Международное сотрудничество в сфере уголовного судопроизводства по делам о преступлениях, совершенных с использованием криптовалюты: постановка проблемы // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования: сб. материалов междунар. науч.-практич. конф. / редкол.: А. В. Гришин [и др.]. – Орел: ОрЮИ МВД России им. В.В. Лукьянова, 2018. – С. 69–70.
16. DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. Official Journal of the European Union. 19.6.2018. L156/43-74.
17. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18

апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.

18. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

Любовь М. В.¹,
студент 5 курса, факультета права
НИУ «Высшая школа экономики»

Научный руководитель:
Пушкарев В. В.,
доцент департамента
уголовного права, процесса и криминалистики
НИУ «Высшая школа экономики»,
кандидат юридических наук, доцент

ТИПОЛОГИЯ И ВИДЫ КОМПЬЮТЕРНЫХ АТАК НА КРЕДИТНЫЕ ОРГАНИЗАЦИИ

Все компьютерные атаки можно разделить на несколько видов в зависимости от метода их осуществления. В качестве основных методов можно выделить эксплуатацию различных уязвимостей программного обеспечения, включающую внешние и внутренние вторжения, применение вредоносного программного обеспечения, а также использование механизмов социальной инженерии. Стоит отметить, что компьютерная атака в редких случаях основана только на одном методе, как правило, это применение сразу нескольких методов, что позволяет преступникам с наибольшей долей вероятности достичь поставленных целей.

Первая группа компьютерных атак основана на эксплуатации различных уязвимостей программного обеспечения кредитных организаций. Атаки могут включать в себя как внешние вторжения, так и атаки со стороны сотрудников, использующих свои привилегированные полномочия. Такие угрозы могут быть реализованы через уязвимости в операционных системах, приложениях для обработки платежей, системах аутентификации и защиты данных. Атаки на уязвимости программного обеспечения могут осуществляться различными методами, среди которых наиболее распространены следующие: атаки «нулевого дня», SQL-инъекции, атаки типа «отказ в обслуживании» и другие.

Уязвимость «нулевого дня», эксплуатация которой относится к атакам «нулевого дня» – это уязвимость, для которой еще не созданы средства защиты и не выпущены обновления системы безопасности. Она не была выявлена в процессе тестирования и остается неизвестной до момента ее эксплуатации. Отличительной чертой уязвимости «нулевого дня» является ее неизвестность на момент использования, что позволяет злоумышленникам проводить скрытые атаки, которые могут привести к серьезным последствиям.

Ключевая опасность уязвимости «нулевого дня» заключается в том, что разработчики еще не знают о ее существовании, и, следовательно, не создали защиту от нее. Злоумышленники могут использовать такую уязвимость для скрытого внедрения в системы и выполнения своих действий, оставаясь незамеченными. После того как будет выпущено обновление, злоумышленники могут

¹ © Любовь М. В., 2025.

продолжить использовать эту уязвимость, но только на тех устройствах, где обновление еще не установлено. После исправления уязвимость перестает быть «нулевым днем».

Преступники могут применять уязвимости нулевого дня для проведения целевых атак на компании или частных пользователей, крадя персональные данные, устанавливая вредоносное программное обеспечение, получая несанкционированный доступ к системам и сетям, а также выполняя другие вредоносные действия [1].

SQL-инъекция (SQLi) представляет собой уязвимость, которая позволяет атакующему внедрять фрагменты вредоносного кода на языке структурированных запросов (SQL), что дает ему возможность манипулировать базой данных и получать несанкционированный доступ к конфиденциальным данным. Атаки, основанные на таких уязвимостях, могут быть нацелены на любое веб-приложение или веб-сайт, взаимодействующие с базой данных SQL.

SQL-инъекции могут быть классифицированы в зависимости от способа получения доступа к данным сервера и возможных масштабов ущерба. Внутриполосная атака представляет собой простой тип атаки, при котором злоумышленник использует один и тот же канал связи для реализации атаки и сбора результатов. Инференциальная атака (или «слепая SQL-инъекция») предполагает, что злоумышленник изучает ответы и поведение сервера после отправки наборов данных, пытаясь извлечь информацию о структуре базы данных. При этом данные не передаются напрямую атакующему, как в случае внутриполосной атаки. Внеполосная атака возникает в тех случаях, когда атакующие не могут получить доступ к данным через один канал связи или когда сервер работает слишком медленно или нестабильно для получения необходимого результата [2].

Последствия успешной SQL-инъекции могут включать не только раскрытие конфиденциальной информации и нарушение безопасности пользователей, но и получение злоумышленниками административного доступа к внутренним системам организации. Согласно данным сообщества Open Web Application Security Project (OWASP), атаки на основе внедрения кода, включая SQL-инъекции, являлись третьим по значимости риском безопасности для веб-приложений в 2021 г. [3].

Следующий тип атак на уязвимости – DDoS-атаки (Distributed Denial of Service) – атаки типа «отказ в обслуживании» представляют собой метод воздействия на сеть, операционную систему или приложение путем перегрузки их огромным объемом трафика, подключений или запросов, превышающих их возможности обработки. Такие атаки могут иметь серьезные последствия для кредитных и иных организаций, включая государственные учреждения.

DDoS-атака является скрытным методом атаки, так как для ее реализации злоумышленнику не требуется административный доступ к сайту или приложению, и такой трафик часто не вызывает подозрений на начальных этапах. Атака инициируется через множество скомпрометированных устройств, находящихся в различных сетях и часто распределенных по всему миру, формируя так называемую бот-сеть. Бот-сеть представляет собой группу устройств, инфицированных вредоносным программным обеспечением. Это отличает DDoS-атаки от атак

типа «отказ в обслуживании» (DoS), при которых используется лишь одно устройство или сеть для осуществления нападения [4].

Вредоносное программное обеспечение (ВПО) – это программы, созданные с целью выполнения несанкционированных действий на устройствах пользователей, включая кражу данных, повреждение систем, вмешательство в работу приложений и многое другое. Существует несколько типов вредоносных программ, каждый из которых имеет свои особенности и методы воздействия. Рассмотрим их подробно:

Троянские программы (или трояны) представляют собой вредоносное ПО, которое маскируется под безвредные или полезные программы, чтобы обмануть пользователя и заставить его установить их. После установки троян начинает выполнять скрытые функции, такие как открытие доступа для злоумышленников к устройству. Преступники могут использовать этот доступ для кражи конфиденциальной информации, управления системой, установки других вредоносных программ или разрушения данных. Основная угроза заключается в том, что трояны часто не вызывают подозрений у пользователя, так как они выглядят как обычные приложения или файлы.

Программы-вымогатели (ransomware) – это тип вредоносного ПО, который блокирует или шифрует данные на зараженном устройстве и требует от жертвы выкуп за их восстановление. Как правило, злоумышленники угрожают удалением данных или их окончательной потерей, если жертва не выполнит требования. Программы-вымогатели могут распространяться через фишинг-атаки, зараженные веб-сайты, вложения в электронные письма или уязвимости в программном обеспечении. Хотя многие жертвы могут быть вынуждены заплатить выкуп, нет гарантии, что преступники вернут доступ к данным. Этот тип ПО представляет собой серьезную угрозу для частных пользователей и организаций, так как может привести к потере важной информации и значительным финансовым убыткам.

Атаки на клиентские устройства включают в себя различные формы злоумышленного воздействия на персональные компьютеры, ноутбуки, смартфоны и другие устройства. Примером может служить установка вредоносных программ через фишинг-атаки или уязвимости в программном обеспечении. Также это могут быть атаки с использованием уязвимостей в веб-браузерах или популярных приложениях, которые позволяют злоумышленникам получать доступ к данным пользователя, мониторить его действия или нарушать работу устройства. Такие атаки часто нацелены на кражу личной информации, финансовых данных или даже паролей от различных аккаунтов.

Зараженные мобильные приложения могут быть установлены пользователями как через официальные магазины приложений, так и через сторонние источники. Эти приложения могут быть замаскированы под полезные утилиты, игры или программы, но после их установки они могут собирать личные данные, такие как пароли, сообщения, данные о местоположении или информацию о банковских счетах. Вредоносные мобильные приложения могут также следить за действиями пользователя, записывать его разговоры или включать камеру и мик-

рофон устройства без его ведома. Существуют также приложения, которые помогают злоумышленникам получать доступ к корпоративным данным, если устройства используются для работы.

Каждый из этих типов вредоносных программ представляет собой серьезную угрозу безопасности как для частных пользователей, так и для организаций, и требует принятия мер по защите от них, включая использование актуальных антивирусных программ, осторожность при скачивании файлов и приложений, а также обеспечение безопасности информационной инфраструктуры.

К отдельной категории, условно отмеченной звездочкой, можно отнести атаки, основанные на методах социальной инженерии. Данный подход отличается от классических компьютерных атак, так как не всегда включает в себя прямое воздействие на информационные системы. Вместо этого злоумышленники манипулируют человеческим фактором, обманывая пользователей и вынуждая их добровольно передавать конфиденциальную информацию или выполнять действия, способствующие компрометации системы. Несмотря на то, что социальная инженерия формально не подпадает под определение компьютерной атаки в традиционном смысле, она остается одним из ключевых инструментов преступников, позволяя им обходить технические меры защиты и получать несанкционированный доступ к информационным ресурсам. В рамках социальной инженерии можно выделить два основных вида атак: вишинг и фишинг.

Вишинг (voice phishing) – это метод социальной инженерии, при котором злоумышленники используют телефонные звонки для обмана жертв и получения от них конфиденциальной информации или денежных средств. Этот тип атак часто направлен на физических лиц, которым представляются сотрудниками банка, правоохранительных органов или других официальных организаций. Основная цель таких звонков – убедить жертву добровольно перевести деньги или предоставить личные данные, такие как коды подтверждения, реквизиты банковских карт, данные паспортов и другие чувствительные сведения.

Существует несколько основных сценариев вишинг-атак. Первый – классический банковский вишинг, который в настоящее время получает вторую жизнь и становится все более популярным. В этом случае злоумышленник звонит жертве, представляясь сотрудником службы безопасности банка, сообщает о подозрительных транзакциях или попытке взлома счета и под предлогом защиты средств убеждает жертву перевести деньги на «безопасный счет», который на самом деле контролируется преступником.

Второй – вишинг с подменой номера. В этом случае используются технологии подмены номера, чтобы звонок выглядел как исходящий от банка, полиции или другой доверенной организации, что увеличивает вероятность того, что жертва поверит мошеннику.

Третий – целевые атаки на сотрудников компаний. Этот сценарий представляется сравнительно новым в методах социальной инженерии, только в последние годы злоумышленники начали активно атаковать не только частных лиц, но и сотрудников организаций, особенно финансовых учреждений и ИТ-компаний. В таких атаках преступники представляются коллегами, техническими специа-

листами или партнерами компании, пытаясь получить доступ к конфиденциальным сведениям. Среди информации, которую они пытаются получить, данные об учетных записях сотрудников, внутренние процедуры безопасности, доступ к корпоративным сервисам и программному обеспечению, а также логины и пароли от внутренних систем.

Четвертый – вишинг с целью распространения вредоносного ПО. Злоумышленники могут убеждать жертву установить на компьютер или смартфон “защитное программное обеспечение”, которое на самом деле является вредоносным ПО, что позволяет атакующим получить полный контроль над устройством жертвы [5].

Эффективность вишинг-атак основана на нескольких факторах. Одним из них является психологическое давление, так как преступники используют методы запугивания, срочности и авторитетности, заставляя жертву принимать решения в состоянии стресса. Технические методы, такие как подмена номера телефона, делают звонок более убедительным. Также важную роль играет недостаточная осведомленность граждан о способах телефонных атак.

Фишинг (phishing) – это один из наиболее распространенных методов компьютерных атак с использованием социальной инженерии, который основан на обмане пользователей с целью получения их конфиденциальных данных, таких как логины, пароли, данные банковских карт и другая чувствительная информация. Атака проводится с использованием поддельных электронных писем, сообщений или веб-сайтов, которые маскируются под официальные ресурсы организаций.

Механизм фишинговой атаки заключается в создании мошеннических сайтов и рассылке писем или сообщений с ложными предложениями, заставляющими жертву перейти по ссылке и ввести свои учетные данные. Чаще всего в таких сообщениях говорится о необходимости срочного подтверждения личности, угрозе блокировки аккаунта, подозрительной транзакции или даже выигрыше в лотерее. Как только пользователь вводит свои данные на поддельном сайте, они сразу же попадают в распоряжение преступников.

Фишинг может принимать разные формы в зависимости от методов распространения и целевой аудитории. Классический фишинг осуществляется через массовую рассылку электронных писем от имени известных организаций, в которых содержатся вредоносные ссылки или вложения. Более сложным вариантом является целенаправленный фишинг, который направлен на конкретных людей или компании. Перед атакой злоумышленники тщательно изучают свою жертву, собирают информацию о ее работе, коллегах и интересах, что делает их сообщения максимально убедительными. Особый подвид такого фишинга – вейлинг (от англ. whale – кит), когда атаки направлены на топ-менеджеров и руководителей компаний с целью получения доступа к корпоративной информации [6].

Согласно ежегодному обзору основных типов компьютерных атак в финансовом секторе, подготовленному Центральным банком Российской Федерации, за 2023 г., основным трендом стало увеличение числа атак, использующих уязвимости в веб-сервисах и системах управления сайтами, а также атак на разработчиков и интеграторов ИТ-решений, применяемых в финансовой сфере. Тем

не менее, наиболее распространенными остаются DDoS-атаки, фишинг, массовые рассылки вредоносных программ и атаки, направленные на перебор паролей с целью компрометации учетных записей [7].

В связи с этим стоит отметить, что в 2024 г. тенденции сохраняются – основными угрозами для кредитных организаций стали: использование уязвимостей, атаки типа «отказ в обслуживании», атаки через скомпрометированные информационные системы подрядных организаций, а также компрометация учетных записей вследствие невнимательности и/или недостаточного контроля за соблюдением политики паролей в информационных системах финансовых организаций [8].

Таким образом, согласно данным Центрального банка, лидерами по количеству инцидентов среди всех видов компьютерных атак стали атаки с использованием метода социальной инженерии и фишинговые атаки.

Список литературы

1. Уязвимости нулевого дня: что это такое и как защититься // СберБанк URL: <https://clck.ru/3EuypU> (дата обращения: 14.03.2025).
2. Что такое SQL-инъекция? Определение и описание // Kaspersky / URL: <https://clck.ru/3K9fYT> (дата обращения: 14.03.2025).
3. OWASP Top 10 – 2021 // OWASP URL: <https://clck.ru/3K9feb> (дата обращения: 14.03.2025).
4. Всяких А. Д. ЧТО ТАКОЕ DDOS-АТАКИ: УГРОЗЫ И ЭФФЕКТИВНЫЕ СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ // Вестник науки. 2024. № 11 (80). URL: <https://clck.ru/3K9g9T> (дата обращения: 14.03.2025).
5. Шинкарук И. П. Вишинг как одна из распространенных форм мошенничества в современном мире / И. П. Шинкарук // За нами будущее: взгляд молодых ученых на инновационное развитие общества: Сборник научных статей 3-й Всероссийской молодежной научной конференции, Курск, 3 июня 2022 года. Том 2. – Курск: Юго-Западный государственный университет, 2022. – С. 285–289. – EDN UKVEWT.
6. Безмалый В. Фишинг, смишинг, вишинг / В. Безмалый // Windows IT Pro/RE. – 2017. – № 10. – С. 59.
7. Обзор основных типов компьютерных атак в финансовой сфере в 2023 году. Департамент информационной безопасности Центрального банка Российской Федерации. // URL: <https://clck.ru/3K9dWn> (дата обращения: 14.03.2025).
8. Обзор основных типов компьютерных атак в финансовой сфере в 2023 году. Департамент информационной безопасности Центрального банка Российской Федерации. // URL: <https://clck.ru/3K9dYu> (дата обращения: 14.03.2025).
9. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

10. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

11. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

12. Пушкарёв, В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

13. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

Вершинина И. О.¹,

*курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Константинов А. В.,

*заместитель начальника кафедры
противодействия преступлениям
в сфере информационно-
телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

КИБЕРБУЛЛИНГ И ЕГО ЗАКОНОДАТЕЛЬНОЕ ЗАКРЕПЛЕНИЕ

Виртуальная травля, или кибербуллинг, стала одной из наиболее острых и актуальных проблем в современном мире, особенно с учетом быстрого развития технологий и повсеместного распространения интернета. Важность этой темы подчеркивается ростом случаев кибербуллинга среди различных возрастных групп, в особенности среди молодежи. Статистика показывает, что значительная часть подростков сталкивается с проявлениями онлайн-агрессии, что влечет за собой серьезные психологические и эмоциональные последствия, такие как депрессивные состояния, тревожность и даже мысли о самоубийстве. В эпоху цифровых технологий, когда большая часть общения перешла в онлайн, необходимо уделять повышенное внимание вопросам защиты пользователей от агрессивного поведения в сети.

Кибербуллинг, как агрессия в цифровой форме, включает в себя оскорбления, запугивания, распространение неправдивой информации и другие действия, цель которых – унижить и преследовать жертву. Необходимо изучить, как разные страны реагируют на эту проблему на законодательном уровне. На международном уровне кибербуллинг не всегда имеет четкое юридическое определение, но многие государства начали разрабатывать и внедрять законы для защиты жертв. В некоторых странах кибербуллинг рассматривается как вид насилия, и последствия могут подпадать под действие уголовного законодательства. Например, в США некоторые штаты приняли законы о кибербуллинге, определяющие это явление и устанавливающие наказания.

В Европе ситуация несколько иная. В некоторых странах, таких как Великобритания, кибербуллинг регулируется существующими законами о защите от преследований и оскорблений. Однако отсутствие специального законодатель-

¹ © Вершинина И. О., 2025.

ства по кибербуллингу создает пробелы в праве, которые могут затруднить привлечение агрессоров к ответственности. В то же время ряд стран, таких как Германия и Франция, начали разрабатывать специальные законы для борьбы с кибербуллингом, включая определение правонарушений и установление санкций.

В России кибербуллинг также не имеет отдельного законодательного регулирования, но его проявления могут подпадать под статьи Уголовного кодекса, касающиеся угроз, разжигания ненависти или вражды, унижения человеческого достоинства и клеветы. В 2019 г. в России был принят Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», который включает меры по борьбе с кибербуллингом. Существующее правовое регулирование в этой области остается недостаточным, что создает пробелы в защите жертв и привлечении агрессоров к ответственности. В частности, стоит подчеркнуть необходимость разработки специальных норм, которые бы четко определяли правонарушения, связанные с буллингом и кибербуллингом, а также устанавливали бы соответствующие санкции.

Законодательное регулирование кибербуллинга – это сложная задача, сопряженная с рядом проблем и недостатков. Основной проблемой является отсутствие четкого определения понятия «кибербуллинг» в законодательстве. Это создает трудности в применении закона, поскольку суды и правоохранительные органы могут по-разному толковать случаи кибербуллинга. Без четких критериев сложно определить, что именно является правонарушением и каковы последствия для нарушителей.

Существующие законы часто отстают от быстро меняющихся технологий и форм общения в интернете. Кибербуллинг может проявляться по-разному, включая оскорбления, угрозы, распространение ложной информации и другие виды агрессии. Однако законодательство, как правило, ориентировано на традиционные формы насилия и агрессии, что делает его недостаточно эффективным в борьбе с новыми вызовами, возникающими в цифровом пространстве. Кроме того, во многих странах кибербуллинг не имеет отдельного статуса в уголовном кодексе, поэтому его проявления часто рассматриваются в контексте других правонарушений, таких как клевета, угрозы или оскорбления. Это может затруднить привлечение виновных к ответственности, поскольку жертвам может потребоваться доказать, что их права были нарушены именно в контексте кибербуллинга, а не в рамках более общих статей.

Также стоит отметить, что законодательство часто не учитывает особенности различных групп населения, таких как дети и подростки, которые наиболее уязвимы к кибербуллингу. Законы о защите несовершеннолетних могут быть недостаточно строгими или эффективными, оставляя жертв без необходимой поддержки и защиты. Важно, чтобы законодательство включало меры по профилактике кибербуллинга в образовательных учреждениях, а также программы обучения как для детей, так и для родителей о рисках и последствиях такого поведения.

Список литературы

1. Проблемы борьбы с буллингом: законодательное решение [Электронный ресурс] // cyberleninka.ru - URL: <https://cyberleninka.ru/article/n/problemy-borby-s-bullingom-zakonodatelnoe-reshenie>.
2. Социально-правовая оценка кибербуллинга [Электронный ресурс] // cyberleninka.ru - URL: <https://cyberleninka.ru/article/n/sotsialno-pravovaya-otsenka-kiberbullinga>.
3. О новых терминах в сфере отечественной правоохранительной деятельности: «киберпреступность» [Электронный ресурс] // cyberleninka.ru - URL: <https://cyberleninka.ru/article/n/o-novyh-terminah-v-sfere-otechestvennoy-pravoohranitelnoy-deyatelnosti-kiberprestupnost>.
4. Юридическая ответственность несовершеннолетних граждан за противоправные действия в сети Интернет (сравнительно-правовой аспект) [Электронный ресурс] // cyberleninka.ru - URL: <https://cyberleninka.ru/article/n/yuridicheskaya-otvetstvennost-nesovershennoletnih-grazhdan-za-protivopravnye-deystviya-v-seti-internet-sravnitelno-pravovoy-aspekt>.
5. Ключевые аспекты дискуссии о законодательном урегулировании буллинга [Электронный ресурс] // cyberleninka.ru - URL: <https://cyberleninka.ru/article/n/klyuchevye-aspekty-diskussii-o-zakonodatelnom-uregulirovanii-bullinga>.
6. Защита детей от кибербуллинга. Вопросы уголовно-правового регулирования [Электронный ресурс] // cyberleninka.ru - URL: <https://cyberleninka.ru/article/n/zaschita-detey-ot-kiberbullinga-voprosy-ugolovno-pravovogo-regulirovaniya>.
7. Проблемы законодательства о киберпреступности [Электронный ресурс] // cyberleninka.ru - URL: <https://cyberleninka.ru/article/n/problemy-zakonodatelstva-o-kiberprestupnosti>.
8. Кибербуллинг как актуальная проблема XXI века [Электронный ресурс] // cyberleninka.ru - URL: <https://cyberleninka.ru/article/n/kiberbulling-kak-aktualnaya-problema-xxi-veka>.
9. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
10. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
11. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
12. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

13. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

14. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Веселова Д. А.¹,
*курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Михайленко Н. В.,
*доцент кафедры противодействия
преступлениям в сфере информационно-
телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

БЕЗОПАСНОСТЬ В ЦИФРОВОМ МИРЕ: ОТ НАИВНОСТИ К ОСОЗНАННОЙ ЗАЩИТЕ

Цифровая трансформация, охватившая все сферы жизни современного общества, привела к ускоренному росту объемов, генерируемых и обрабатываемых данных, а также к расширению возможностей использования информационно-телекоммуникационных технологий (далее – ИКТ). Вместе с тем развитие цифрового пространства породило новые вызовы и угрозы, связанные с ростом числа преступлений в сфере ИКТ. Недостаток знаний о методах киберпреступников и недостаточная осведомленность о последствиях небрежного обращения с личными данными приводили к многочисленным случаям мошенничества, кражи личной информации и заражения вредоносными программным обеспечением. Сегодняшний мир, в условиях постоянного усложнения киберугроз и увеличения их масштабов, требует осознания необходимости активной и комплексной защиты в цифровом мире, что будет являться значительным фактором обеспечения безопасности как отдельных пользователей, так и организаций, и государства в целом [2].

Наивность пользователей, проявляющаяся в отсутствии элементарных знаний о правилах безопасного поведения в Интернете, стала одной из главных причин роста киберпреступности. Часто пользователи переоценивают защищенность своих данных, что приводит к грубым ошибкам, таким как использование одинаковых паролей для разных аккаунтов, игнорирование двухфакторной аутентификации и отсутствие обновлений программного обеспечения. Наивный подход к безопасности информации также проявляется в неосознанном доверии к источникам информации, что делает устройства уязвимыми для фишинговых атак и манипуляций.

За последние десятилетия ландшафт угроз в цифровом мире претерпел значительные изменения. Если на начальном этапе основными рисками являлись

¹ © Веселова Д. А., 2025.

вирусные атаки и спам, связанные с массовым распространением персональных компьютеров по всему миру, то в настоящее время спектр угроз значительно расширился и включает:

1. Фишинг. Мошеннический метод, который был создан для получения конфиденциальной информации пользователей путем обмана и манипуляций. Статистический анализ, проведенный с помощью открытых отчетов организаций, наглядно демонстрирует, что фишинговые атаки выросли за период 2024 года на 34 % по сравнению с предыдущим. Более 70 % организаций сообщили, что они стали жертвами фишинга.

2. Вредоносное программное обеспечение (ВПО). Различные программы, предназначенные для нанесения ущерба компьютерным системам, кражи данных и нарушения их работоспособности. Чаще всего жертвами становятся медицинские учреждения, научные и образовательные организации и промышленные предприятия.

3. Атаки на веб-приложения. Использование уязвимостей на веб-сайтах и приложениях для получения несанкционированного доступа к данным и выполнения вредоносных действий. Первый квартал 2025 года, по данным группы компаний «Солар», зафиксировал 800 млн веб-атак на сайтах российских компаний, который чаще всего осуществлялись с помощью ботов.

4. Кибершпионаж. Несанкционированный доступ к информации с целью получения коммерческой или политической выгоды. Осуществление противоправных действий с помощью скрытого мониторинга в 2024 года по информации «Информзащита» составило 58 %, атаки чаще всего были направлены на промышленный сектор и розничную торговлю, что в очередной раз подтверждает большой уровень уязвимости в данных сетях [4].

5. Распространение дезинформации и фейковых новостей. Создание и распространение ложной информации с целью манипулирования общественным мнением и дестабилизации политической обстановки. Чаще всего недостоверная информация находится в социальных сетях и мессенджерах, пользователи вводят личные данные и лишь спустя время понимают, что стали жертвой мошенничества.

Эти угрозы представляют собой серьезную опасность для всех участников цифрового пространства, от отдельных пользователей до крупных организаций и государственных структур. Для эффективного противодействия современным киберугрозам необходим комплексный подход, включающий такие компоненты, как: технические средства защиты, организационные меры, правовое регулирование, образование и просвещение. Рассмотрим более подробно каждый ранее упомянутый компонент.

Технические средства защиты включают в себя использование антивирусного программного обеспечения, систем обнаружения и предотвращения вторжений, средств шифрования данных и других технических инструментов для защиты компьютерных систем, и сетей. Специальные устройства, обеспечивают шифрование информации, защищают от несанкционированной обработки, доступа и хранения при обмене по каналам связи.

Организационные меры направлены на разработку и внедрение политик безопасности, регламентирующих правила работы с информацией, процедуры доступа к данным, методы контроля и мониторинга безопасности. Анализ сетевой активности позволяет считывать объем трафика и типы передаваемых данных, с помощью чего возможно выявить аномалии, указывающие на конкретную веб-атаку.

Правовое регулирование как компонент эффективного противодействия киберугрозам будет полностью реализован только в случае разработки и совершенствования законодательства в области кибербезопасности, установлению ответственности за совершение киберпреступлений и нарушение правил защиты данных.

Образование и просвещение, направленное на повышение уровня цифровой грамотности и осведомленности пользователей о рисках и угрозах в цифровом мире, формирование культуры в киберпространстве и осознанного отношения к защите информации и личных данных.

Ключевым фактором повышения уровня кибербезопасности является формирование цифровой грамотности и осознанного отношения к информационной безопасности у пользователей всех возрастов [7]. Клиенты при использовании обширной сети Интернет должны знать основные принципы безопасного поведения, уметь распознавать фишинговые атаки и вредоносные программы, использовать сложные пароли и защищать свои учетные записи. Пользователи с помощью развития критического мышления должны уметь анализировать информацию, поступающую из Интернета, отличать достоверные источники от ложных новостей и не поддаваться на манипуляции. Также у каждого должно быть сформировано понимание, какие данные он предоставляют на сайтах, кому они могут быть доступны и как их могут использовать. Важно, чтобы пользователи понимали, что безопасность в цифровом мире – это не только технические средства, но и их личная ответственность.

Эффективное правовое регулирование выполняет значительную роль в обеспечении безопасности в цифровом мире. Законодательство должно определять:

- права и обязанности пользователей и организаций в области защиты информации;
- ответственность за совершение киберпреступлений;
- полномочия правоохранительных органов в сфере борьбы с киберпреступностью;
- правила обработки и защиты персональных данных.

Развитие правового регулирования в области кибербезопасности должно учитывать современные тенденции и новые технологии, а также соответствовать международным стандартам.

В заключение следует подчеркнуть, что безопасность в цифровом мире – это сложная и многогранная проблема, требующая комплексного подхода. Переход от наивного подхода к осознанной защите предполагает повышение осведомленности пользователей о потенциальных рисках, формирование культуры кибербезопасности, использование современных технических средств защиты, а также совершенствование законодательства и правоприменительной практики в сфере

борьбы с преступностью ИКТ. Важно помнить, что в условиях стремительного развития технологий каждый из нас несет ответственность за свою безопасность и безопасность окружающих в цифровом мире. Только совместные усилия государства, правоохранительных органов и пользователей позволят обеспечить безопасное и комфортное использование информационно телекоммуникационных технологий и построить защищенное общество.

Список литературы

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
2. Агапов А. Б. Информационная безопасность в России: правовые основы: учебное пособие для студентов вузов / А. Б. Агапов. — М.: Издательство «Юрайт», 2014. — 336 с.
3. Галатенко В. А. Основы информационной безопасности: учебное пособие для вузов / В. А. Галатенко. — М.: Издательство «Гардарики», 2004. — 208 с.
4. Галушкин А. А. К вопросу о кибершпионаже и киберконтрразведке на современном этапе // Вестник РУДН. Серия: Юридические науки. 2014. № 3. — 4 с.
5. Захарова В. Д. Кибербезопасность в цифровом пространстве// Экономика и управление: опыт и новые решения в эпоху трансформаций. 2023. № 1. — 7 с.
6. Информационное право: учебное пособие/ [Я. В. Барченкова и др.]. М., 2024.
7. Токтарова В. И., Ребко О. В. Цифровая грамотность: понятие, компоненты и оценка // Вестник Марийского государственного университета. 2021. № 2 — 4 с.
8. Щербак А. В. Информационная безопасность: учебник для вузов / А. В. Щербак. — 2-е изд. — Москва: Издательство Юрайт, 2023. — 252 с.
9. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 263 с. — ISBN 978-5-4497-4085-4. — EDN FGPMCO.
10. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 197 с. — ISBN 978-5-4497-4146-2. — EDN UICMXX.
11. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. — Москва : Ай Пи Ар Медиа, 2025. — 167 с. — ISBN 978-5-4497-4056-4. — EDN TGFRRN.
12. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. — 62 с. — ISBN 978-5-4497-3726-7. — EDN FJISXZ.
13. Михайленко Н. В. Перспективы и проблемы отправления цифрового правосудия в Российской Федерации / Н. В. Михайленко // Закон и право. — 2020. — № 4. — С. 201–205.

Власова Я. Э.¹,

*курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В. Я. Кикотя*

Научный руководитель:

Поликарпова Е. В.,

*старший преподаватель кафедры
противодействия преступлениям
в сфере информационно-
телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

УРОВЕНЬ ЦИФРОВИЗАЦИИ В ОБЩЕСТВЕ И РАЗВИТИЕ В НЕМ КИБЕРПРЕСТУПНОСТИ

Цифровизация общества, которая охватывает Интернет, мобильные устройства, умные устройства (ИИ), приносит достаточную выгоду в виде улучшенного доступа к услугам и сервисам, а также экономический рост. Однако, как показывает практика, цифровизация имеет другую сторону медали, связанную с ростом киберпреступности. Чаще всего в киберпреступность входит фишинг, взломы, программа-вымогатель. В этой статье мы рассмотрим, как уровень цифровизации влияет на развитие киберпреступности и обсудим возможные меры для ее предотвращения.

Киберпреступление – криминальная активность, включающая использование компьютерных сетей (включая Интернет) как основного средства совершения преступления. Это тип криминальной активности, которая включает в себя использование компьютерных сетей (включая Интернет) в качестве основного средства совершения преступления [1]. По прогнозам, к 2025 году количество подключенных устройств превысит 75 млрд по всему миру. В России ущерб от киберпреступлений в 2024 году вырос на 36 % по сравнению с 2023 годом и составил 200 млрд рублей, но вместе с этим число пострадавших осталось почти неизменным [2].

Одной из причин роста киберпреступности может быть низкая киберграмотность, особенно в России: она делает людей более уязвимыми к интернет-мошенничествам. Ежедневно в России фиксируется от 6 до 7 млн мошеннических звонков, и их количество остается на том же уровне несколько месяцев [3]. Об этом заявил заместитель председателя правления Сбербанка в апреле 2025 года на выступлении в Совете Федерации. Для борьбы с киберпреступностью необходимы усилия на разных уровнях: это включает модернизацию систем защиты, повышение киберграмотности через образовательные программы.

¹ © Власова Я. Э., 2025.

Второй причиной может быть количество подключенных устройств к сети Интернет. Чем больше их подключено, тем больше возможностей атаковать эти устройства.

Третья причина – увеличение объема данных. В цифровизированном обществе все чаще информация хранится электронно: это могут быть как персональные данные, так и финансовые данные и многое другое. Однако на данный момент уже существуют пути решения борьбы с киберпреступлениями.

Все чаще с населением проводят профилактические работы, как реагировать на мошенничество и что следует делать в тех или иных ситуациях, что позволяет минимизировать киберпреступления.

В образовательные программы вводят борьбу с киберпреступлениями, что также поднимает киберграмотность.

Создаются программы на различные устройства для защиты от взлома и копирования персональных данных.

Службы безопасности намного чаще находят кибермошенников благодаря разработанным методикам, которые они улучшают, то есть делают менее уязвимыми к атакам и доступу в программы.

Искусственный интеллект уже не только генерирует запросы, но и настроен на защиту и выявление подозрительных операций в сети.

В России также предпринимаются шаги для повышения кибербезопасности. Например, поднимаются вопросы по модернизации устаревших систем, внедрению новых методов защиты и активному обмену информацией об угрозах между организациями.

Эксперты отмечают, что уголовно-процессуальное право не совсем адаптировано для борьбы с атаками данного вида преступлений, и вместе с этим на данный момент правоохранительным органам не хватает специалистов в данной сфере.

Атаки становятся более продвинутыми: киберпреступники остаются незамеченными в IT-инфраструктуре месяцами, и атаки на критическую информационную инфраструктуру занимают седьмое место по вероятности глобальных угроз, с прогнозируемым экономическим ущербом в 8–10 триллионов долларов США.

В заключение стоит отметить, что цифровизация открывает перед обществом огромные возможности, но одновременно создает новые риски, связанные с киберпреступностью. Рост числа подключенных устройств, увеличение объема данных и доступность инструментов для атак делают киберугрозы все более значительными. Для минимизации этих рисков необходим комплексный подход, включающий усиление кибербезопасности, повышение осведомленности населения, международное сотрудничество и развитие новых технологий защиты. Только совместными усилиями можно обеспечить безопасное цифровое будущее, в котором преимущества цифровизации будут преобладать над ее рисками.

Список литературы

1. Виды киберпреступлений [Электронный ресурс] URL: <https://cisoclub.ru/vidy-kiberprestuplenij/> (дата обращения: 10.05.2025).

2. Ущерб от IT-преступлений в 2024(ТАСС) [Электронный ресурс] URL:<https://tass.ru/obschestvo/23183001> (дата обращения: 10.05.2025).
3. Телефонное мошенничество [Электронный ресурс] URL:<https://www.tadviser.ru/index.php> (дата обращения: 10.05.2025).
4. Виноградова Е. В., Полякова Т. А., Минбалеес А. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. – 2021. Т. 5. № 4. С. 5–19.
5. Проблемы создания цифровой экосистемы: правовые и экономические аспекты / Е. Н. Абрамова, С. Н. Белова, В. А. Вайпан [и др.]. – М.: Юстицинформ, 2021. С. 276.
6. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. (2021). Цифровая криминология: учебное пособие. Москва: Академия управления МВД России.
7. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
8. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
9. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
10. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
11. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.
12. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.
13. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Волкова Ю. А.¹,

*курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Константинов А. В.,

*заместитель начальника кафедры
противодействия преступлениям
в сфере информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ПОНЯТИЕ И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ DARKNET

DarkNet (далее – Даркнет) зачастую называют «черным» или «теневым» интернетом. Суть заключается в его скрытности, отсутствия доступа без специализированных инструментов (браузеров). Помимо того, Даркнет гарантирует стопроцентную анонимность между пользователями, устанавливая не открытое соединение, а зашифрованное.

Так, например, Даркнет использует собственные адреса ресурсов. Благодаря этому невозможно индексировать сайты, зайти через стандартный поисковик.

Исследователи классифицируют сеть на три вида:

1. Видимый интернет.
2. Глубинный интернет.
3. Даркнет.

В первых двух классах мы можем наблюдать сайты с общим доступом или частным. Частный доступ сайтов доступен для «глубинного» интернета. Ресурсы в данной категории сети, как и в Даркнете, нельзя индексировать. Получение доступа к материалам, размещенным в «глубинном» интернете, возможно лишь при наличии логина и пароля. Даркнет, в свою очередь, помимо этого, использует специальные софты, о чем было сказано ранее [1].

Интерес в данном контексте представляют способы, используемые для входа в «черный интернет». Наиболее распространенным является браузер «Tor», который является источником наибольшего количества теневых ресурсов. Говоря о нем подробнее, отметим, что разработка указанного браузера происходила в конце девяностых с целью засекречивания переговоров спецслужб под руководством Научно-исследовательской лаборатории Военно-морских сил Соединенных штатов Америки. Со временем данный проект стал открытым. На сегодняшний день его работа осуществляется с помощью команды «Tor Project».

¹ © Волкова Ю. А., 2025.

Второе место занимает сервис – сеть «I2P». Данный сегмент содержит меньшее количество ресурсов, нежели «Tor». Его плюс заключается в большей безопасности и анонимности, поскольку сеть «I2P» изначально проектировалась как сеть для посещения скрытых сайтов [2].

Эксперт «Лаборатории Касперского» Дмитрий Галов в одном из интервью отметил, что само посещение Даркнета не является противозаконным, важно понимать, какую цель преследует пользователь. Даркнет сам по себе не является источником лишь противоправного контента. В нем можно найти нейтральные аналоги сетей для переписки, форумы. Однако Галов замечает, что основная масса активности принадлежит именно злоумышленникам.

Даркнет располагает сервисами, позволяющими незаконно приобрести запрещенные товары. Это и оружие, и наркотики, и фальшивые деньги. Данная сеть развивается также и в контексте противоправных услуг, можно заказать даже убийство. Инсайдерская информация, базы данных – это можно найти в «черном интернете». И все это мирно уживается с обыденными для нас сервисами – почта, социальные сети, онлайн-библиотеки, различные форумы [3].

Легальные ресурсы порой тоже размещаются в сети Даркнет. Так, например, в 2014 году Facebook (признано экстремистской организации и запрещена в Российской Федерации) зарегистрировал в «Tor» свою версию сайта.

Самыми популярными услугами в Даркнете считаются покупки баз данных пользователей, взломы аккаунтов в мессенджерах, оформление фальшивых документов, отмывание денежных средств за определенный процент и другие [4].

Покупка баз данных не случайно стоит на первом месте в списке перечисленных – это наиболее популярная мошенническая схема. Сначала происходит взлом сервисов, откуда копируется вся необходимая информация, затем она подлежит размещению на специализированных форумах за конкретную стоимость.

Как ранее было отмечено, сервис гарантирует полную анонимность своих пользователей. Это возможно благодаря отсутствию хранения логов, игнорирования запросов органов власти, усложнения собственной инфраструктуры и постоянное поддержание и увеличение уровня конспирации. Постоянные пользователи, помимо того, ведут себя достаточно осторожно, подключая VPN, который позволяет скрыть местоположение, а также не указывают своих личных данных [5].

Даркнет отрицает законодательство всех стран, но в рамках платформы все же существует перечень правил и требований к участникам. Как и на обычных форумах, сеть имеет своих модераторов, контролирующих поведение и взаимодействие пользователей. Для гарантированности сделок между ними существует третье лицо, обладающее определенным авторитетом, который должен убедиться в том, что предложенный товар или услуга обладают заявленными характеристиками. Если в Даркнет происходит спор, то он подлежит разрешению в рамках арбитража.

Говоря об анонимности, отметим такую характерную особенность, как условность. Если пользователь самостоятельно размещает в рамках сервиса свои данные, тогда за свою безрассудность он отвечает самостоятельно. В этом тоже есть определенная разница между общедоступными сервисами и даркнетом. Первые,

работая над своей репутацией, относятся с «заботой» о своих участниках в то время, как пользователи даркнета наиболее уязвимы.

Злоумышленники стараются держаться современных трендов и, если услуга становится неактуальной, просто снимают ее с продажи, заменяя ее на что-то более востребованное. Так, например, «Лаборатория Касперского» проанализировала определенную закономерность: при появлении угрозы коронавирусной инфекции злоумышленниками сразу были опубликованы объявления, связанные с продажей нескольких видов вакцин. Когда же у некоторых людей появились сомнения в эффективности вакцинирования, а сама процедура во многом стала обаятельной – мошенники предложили услугу по фальсификации медицинских справок, свидетельствующих о прохождении необходимых мероприятий [6].

Многие исследователи «теневого интернета» хотя бы раз, но задавались вопросом о возможности блокировки Даркнета. На мой взгляд, на сегодняшний день это невозможно. Проводятся различные меры по ограничению доступа к браузеру «Тор», однако попытки безуспешны, в силу технической невозможности адресной блокировки конкретных сайтов в Даркнете. Политика Российской Федерации в области ограничения началась в декабре 2021 года, однако спустя практически неделю, блокировка сети была снята.

У правоохранительных органов давно сложилось понимание того, что сам по себе «Тор» обладает огромным количеством путей обхода, поэтому дальнейшая деятельность в этом направлении бессмысленна. Сегодня стоит задача по усложнению использования указанного браузера, с целью снижения криминогенной ситуации [7].

Список литературы

1. Варданян А. В. Оборот наркотических средств и психотропных веществ в учреждениях системы здравоохранения как объект научного анализа.
2. Демко Н. М. Криптомаркеты – анонимные онлайн-рынки распространения наркотиков.
3. Интернет-преступления, виды и превентивные меры [Электронный ресурс].
4. Исаков Р. В. О противодействии легализации (отмыванию) наркодоходов с использованием финансовых активов (криптовалют).
5. Преступления в сфере незаконного оборота наркотиков и их предупреждение [Электронный ресурс].
6. Преступления в сфере незаконного оборота наркотиков и их предупреждение [Электронный ресурс].
7. Преступления в сфере незаконного оборота наркотиков и их предупреждение [Электронный ресурс].
8. Узденов Р.М. Новые границы киберпреступности.
9. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

10. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
11. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
12. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
13. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.
14. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Воронкова М. В.¹,
студент 2 курса магистратуры,
факультет права
НИУ «Высшая школа экономики»

Нуреев Д. О.²,
студенты 2 курса магистратуры,
факультет права
НИУ «Высшая школа экономики»

Научный руководитель:
Пушкарев В. В.,
доцент департамента уголовного права,
процесса и криминалистики
НИУ «Высшая школа экономики»,
кандидат юридических наук, доцент

ПРАВОВОЕ РЕГУЛИРОВАНИЕ КРИПТОВАЛЮТЫ В ЕВРОПЕЙСКОМ СОЮЗЕ

Появление новых технологий и их внедрение в экономику трансформирует ее и повышает конкурентоспособность той экономической системы, которая в самое быстрое время сможет воспользоваться преимуществами, которые эти технологии за собой несут. Функционирующая на основе блокчейна криптовалюта навсегда изменила мировой финансовый рынок, внося существенные коррективы в соотношение финансовых инструментов на нем. Актуальность вопросов, связанных с правовым регулированием криптовалюты возрастает по мере созревания и развития нового финансового рынка, результатом которой становится независимая и, порой, неподконтрольная государству финансовая система.

Европейский союз имеет одну из крупнейших криптоэкономик в мире [1]. Первые заявления о необходимости правового регулирования криптоактивов делались европейскими политиками и государственными органами более десяти лет назад – в 2013 г. Европейская банковская организация сделала публичное заявление о рисках, связанных с оборотом криптовалюты [2]. Спустя 10 лет публичных обсуждений в Европейском союзе был принят закон, вводящий нормативную базу для правового регулирования криптоактивов – Регламент (ЕС) 2023/1114 Европейского парламента и Совета от 31 мая 2023 года о рынках криптоактивов (далее – MiCA или Регламент) [3].

На мировом уровне MiCA представляет собой наиболее передовое законодательство о криптоактивах на сегодняшний день. Закон устанавливает всеобъемлющий набор требований к пруденциальному и поведенческому регулированию эмитентов и оферентов криптоактивов, а также поставщиков услуг криптоактивов. Он также предоставляет обширные регулирующие полномочия надзорным

¹ © Воронкова М. В., 2025.

² © Нуреев Д. О., 2025.

органам для обеспечения финансовой стабильности по отношению к присущей рынкам криптоактивов волатильности.

Целью настоящей статьи является систематизация и анализ основных положений MiCA и оценка влияния MiCA на рынок криптоактивов в ЕС и во всем мире. Авторы статьи также проанализировали критические позиции, высказываемые экспертами в адрес MiCA.

MiCA применяется в отношении «криптоактивов», которые определяются как «цифровое представление ценности или права, использующее криптографию для безопасности и имеющее форму монеты или токена или любого другого цифрового носителя, который может передаваться и храниться в электронном виде, с использованием технологии распределенных реестров или аналогичной технологии», которые классифицируются на три вида: Asset Reference Token («ART»); E-money Token («EMT»); другие криптоактивы как «цифровое представление стоимости или прав, которые могут передаваться и храниться в электронном виде».

Сфера действия MiCA по кругу лиц включает следующих субъектов: физические или юридические лица, которые выпускают криптоактивы («эмитенты», «issuers»); физические или юридические лица, которые предлагают криптоактивы публике («оференты», «offerors»); физические или юридические лица, которые предоставляют одну или несколько из следующих услуг на профессиональной основе: (i) хранение и администрирование криптоактивов от имени третьих лиц; (ii) работа торговой платформы; (iii) обмен на средства; (iv) обмен криптоактивов на другие криптоактивы; (v) выполнение заказов на криптоактивы от имени третьих лиц; (vi) размещение криптоактивов; (vii) передача криптоактивов от имени третьих лиц; (viii) прием и передача заказов на криптоактивы от имени третьих лиц; (ix) предоставление консультаций по криптоактивам; (x) предоставление управления портфелем криптоактивов («поставщики услуг криптоактивов», «crypto-asset service providers»).

MiCA устанавливает базовый режим для всех эмитентов криптоактивов вне зависимости от их видов и дополнительные требования к эмитентам токенов, привязанных к активам («ART»), и эмитентов токенов электронных денег («EMT»). Базовый режим включает в себя: обязательную регистрацию в качестве юридического лица в ЕС; разработку и принятие «Белой книги» с описанием условий осуществления деятельности; уведомления уполномоченного органа о принятии «Белой книги».

В отношении эмитентов токенов, привязанных к активам, действуют дополнительные требования к получению лицензии в ЕС, организационной структуре внутри компании, созданию системы идентификации, управления и отчетности о рисках, связанных с выпуском криптовалюты. Такие эмитенты также должны разработать план восстановления на случай реализации рисков, в частности иметь резервные активы. В отношении эмитентов токенов электронных денег установлены следующие требования: такая деятельность доступна только кредитным организациям и организациям электронных денег, осуществляющим деятельность в соответствии с законодательством ЕС. Такие лица обязаны уведомить уполномоченный орган о своем намерении осуществлять выпуск токенов

электронных денег за сорок дней до начала выпуска и предоставить в распоряжение уполномоченного органа «Белую книгу» за двадцать дней до начала выпуска токенов [4].

Как следует из указанных выше положений, регулирование эмиссии криптоактивов направлено, в первую очередь, на защиту потенциальных инвесторов и накладывает существенные ограничения на деятельность эмитентов, а в некоторых случаях – и вовсе препятствуют выходу на рынок огромного числа субъектов, как в случае с эмитентами токенов электронных денег, которыми могут быть только кредитные организации и организации, осуществляющие операции с электронными деньгами.

Второй основной группой лиц, на которую распространяет свое действие MiCA, является группа провайдеров услуг с использованием криптоактивов, под которой понимается любая услуга или деятельность, относящаяся к криптоактивам. Провайдеры услуг должны соответствовать большому количеству требований, в частности, иметь специальную лицензию (за исключением уже имеющих лицензию кредитных организаций и инвестиционных фирм), зарегистрировать офис в ЕС, разработать систему управления рисками, мониторить и раскрывать конфликты интересов и проводить KYC клиентов, раскрыть тип используемых блокчейн технологий в Белой книге по аналогии с эмитентами криптоактивов, иметь гарантии для клиентов в виде резервного капитала или страхования ответственности.

Одним из наиболее дискуссионных моментов при принятии Регламента стало введение ответственности провайдеров услуг хранения и управления криптоактивов от имени третьего лица за возможные потери. Такой провайдер обязан вернуть идентичные активы или их стоимость эмитенту, если они были утрачены, за исключением тех случаев, когда утрата произошла в результате форс-мажора. Если утрата произошла по причине некачественного оказания услуги, провайдер такой услуги несет ответственность в пределах рыночной стоимости утраченных криптоактивов.

При этом под хранением криптоактивов и управлением ими от имени третьего лица понимается осуществление любого контроля над криптоактивами. Такое широкое понимание хранения к криптоактивам делает применение правила об ответственности за потери применимым к большому числу субъектов [5]. В связи с этим данное правило может потенциально сильно сузить круг субъектов, предлагающих услуг по хранению криптоактивов в ЕС [6].

Одной из целей MiCA является обеспечение высокого уровня защиты прав потребителя. Ключевыми мерами по защите прав потребителей, предусмотренные MiCA, являются: обязательное информирование потребителей компаниями об особенностях функционирования криптоактива (в Белой книге), обо всех сборах, взимаемых провайдером услуг с использованием криптоактива, а также о рисках, связанных с инвестированием; все маркетинговые коммуникации, касающиеся предложения криптоактива общественности или допуска его к торговле, должны соответствовать определенным требованиям, в частности: (i) быть справедливыми, понятными и не вводить в заблуждение, (ii) быть идентифицируемыми как таковые и (iii) соответствовать техническому документу; обязанность

эмитентов криптоактивов поддерживать собственные средства на определенном уровне и иметь резервные активы, обеспечивающие требования к эмитенту и др.

MiCA предусматривает двухуровневую систему контроля за соблюдением его положений. На первом уровне расположены национальные уполномоченные органы – они осуществляют надзор за соблюдением положений MiCA большинством эмитентов криптоактивов и провайдеров услуг с использованием криптоактивов. Второй уровень системы принадлежит Европейскому ведомству по криптоактивам и ценных бумаг.

Для провайдеров услуг, имеющих более пятнадцати миллионов активных пользователей (значительных провайдеров услуг), национальные органы также остаются контрольными органами, однако Европейское ведомство по рынкам криптоактивов и ценных бумаг имеет право самостоятельно запретить или ограничить деятельность провайдера услуг с использованием криптоактивов, если такая деятельность представляет собой угрозу стабильности и целостности рынка или инвесторам. Также Европейское ведомство по рынкам криптоактивам и ценных бумаг будет выпускать разъяснения по применению MiCA.

В отношении стейблкоинов, которые имеют более десяти миллионов пользователей, контрольные функции, помимо Европейского ведомства по рынкам криптоактивов и ценных бумаг, будет также осуществлять Европейская банковская организация. Полномочия Европейской банковской организации включают возможность наложить вето на какие-либо операции со стейблкоинами.

Европейское ведомство по криптоактивам и ценным бумагам также будет вести черный список криптоактивов. Провайдеры услуг с использованием криптоактивов, которые не соблюдают требования Регламента, будут включены в данный список. Последствия включения в список состоят в том, что инвесторы будут уведомлены о несоблюдении провайдеров законодательства и высоких рисках, связанных с инвестированием в данную криптовалюту.

В MiCA также предусмотрено ряд мер, направленных против злоупотребления правами на рынке криптоактивов. Они, в частности, включают требования, касающиеся раскрытия внутренней информации, запрет на инсайдерские сделки, запрет на незаконное раскрытие внутренней информации и запрет на манипулирование рынком. Данные меры во многом дублируют меры по предотвращению злоупотреблений, предусмотренные европейским законодательством о ценных бумагах.

В краткосрочной перспективе ожидается, что внедрение MiCA, вероятно, приведет к увеличению затрат на соблюдение нормативных требований для криптовалютных компаний в целях соблюдения новых правил [7]. Эксперты также прогнозируют замедление роста или исключение из листинга некоторых криптовалют в связи с потенциальными регуляторными рисками [8]. Нельзя не отметить, что USDT является одним из самых ликвидных и востребованных стейблкоинов в мире, поэтому исключение USDT из листинга вызвало негативную реакцию и привело к прогнозам о возможном падении криптовалютного рынка ЕС [9].

В долгосрочной перспективе ожидается, что MiCA создаст более стабильный и прозрачный рынок криптовалют в Европе, обеспечит правовую определенность в регулировании криптовалют в ЕС. Это может способствовать инновациям и росту в европейском секторе и позиционированию ЕС как лидера на мировом рынке криптовалют [10].

Отдельно стоит отметить, что принятие MiCA позитивно скажется на предотвращении финансовых преступлений с использованием криптовалют за счет того, что содержит требования по борьбе с отмыванием денег, а также обязательное проведение процедуры KYC, что затрудняет преступникам использование криптовалюты в незаконных целях. Стоит также отметить, что принятие MiCA значительно увеличивает легитимность криптовалют в ЕС, а следовательно - доверие к ним. В связи с этим, принятие MiCA также повышает интерес к криптовалютам потребителей и инвесторов.

Тем не менее принятие MiCA может привести к сокращению компаний, занимающихся эмиссией или оказанием услуг с использованием криптовалюты, в связи с тем, что новые регуляторные требования несут затраты, которые могут быть не под силу небольшому бизнесу. По оценкам экспертов, можно ожидать, что криптобизнес в ЕС сосредоточится в больших компаниях, а стартапы и небольшие компании предпочтут релокацию за пределы ЕС [10].

Кроме того, обязанность по регистрации компании в ЕС, предусмотренная как для эмитентов криптовалюты, так и для провайдеров услуг с использованием криптовалюты, может дестимулировать ряд компаний вести деятельность на европейском рынке, что может также негативно сказаться на росте рынка криптовалюты в Европе.

При этом некоторые эксперты считают, что принятие MiCA, хотя и приведет к оттоку стартапов из криптоиндустрии, может привести к выходу на крипторынок больших компаний, которые раньше боялись выходить на данный рынок из-за отсутствия четкого регулирования и сопутствующих этому репутационных рисков. Альтернативным сценарием может стать увеличение поддержки стартапов со стороны больших компаний, что позволит сохранить присутствие стартапов и небольших компаний на европейском рынке [11].

Среди других недостатков MiCA отмечается его пробельность в отношении услуг криптокредитования, которые влекут за собой существенные риски мошенничества и нарушений прав потребителей [12, с. 521]. Как было отмечено выше MiCA регулирует только услуги по хранению криптовалюты и не содержит положений, посвященных кредитованию с использованием криптовалюты. При этом в соответствии с MiCA провайдеры таких услуг не вправе брать проценты за предоставление услуг – данный запрет вызвал негативную реакцию некоторых экспертов в связи с отсутствием разумных причин его установления. Вероятно, установление подобного запрета обусловлено политическими соображениями, направленными на снижение риска использования стейблкоинов в качестве средства сбережения и обеспечение финансовой стабильности за счет снижения конкуренции между традиционными банковскими депозитами и стейблкоинами, особенно в текущих условиях низких процентных ставок [12, с. 523].

Будучи первым всеобъемлющим законодательным актом в ЕС в сфере криптоактивов, MiCA безусловно играет большую роль в формировании европейского криптоландшафта. MiCA содержит подробные требования к эмитентам криптовалют и провайдерам услуг с использованием криптовалют, нацеленные на защиту инвесторов и потребителей, предотвращение финансовых преступлений и иных злоупотреблений с использованием криптовалют, что в конечном счете может привести к созданию более стабильного, прозрачного рынка, формированию правовой определенности, повышению доверия инвесторов и государственных органов к криптовалютам. Ожидается, что подобная правовая определенность также принесет больше уверенности в секторе и поможет развитию стратегических криптопроектов [13].

Тем не менее принятие MiCA не лишено недостатков, в частности, MiCA предусматривает требования, слишком обременительные для стартапов и небольшого бизнеса, а также снижает уровень анонимности, традиционно ассоциирующейся с криптовалютами, что может негативно сказаться на развитии инноваций в европейской криптовалютной индустрии. Отмечается также, что очень низкий порог в 1000 евро для отчетности приводит к усилению наблюдения и большой перечень действий, которые подпадают под разрешительный порядок, приведет к ограничениям в криптоиндустрии, а с учетом того, что в других юрисдикциях, например, в США, не предусмотрены такие строгие правила для рынка, европейские компании могут сменить свою юрисдикцию, что повлечет за собой негативное изменение европейского инвестиционного климата [14].

Несмотря на некоторые минусы, принятие MiCA является важнейшим шагом для криптовалютной индустрии как в ЕС, так и во всем мире. С большой вероятностью, MiCA будет взят за основу при разработке национальных законов о криптовалютах в странах, не входящих в ЕС, в частности в России.

Список литературы

1. DeFi makes Western Europe the world's largest 'crypto economy' // Yahoo.Finance. [Электронный ресурс]. URL: https://finance.yahoo.com/news/de-fi-made-western-europe-the-worlds-largest-crypto-economy-170824285.html?guc-counter=1&guce_referrer=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAEFT0BodTXG26mPun4m_W6OtlfafXO4NUFGsgPdqn3IwCvqNImXfPXp1_idYoEPufcZIt-HskTM2RVc2QtRYys-LsuEu5RvJjwqFV4oa_QqHTXWn0JL52b0K80wNIq6tqlg3WCFYh-FIPt72J1Hfj8Qv2pgc6TKlSMF_W5ici3P3 (дата обращения: 02.02.2025).
2. EBA Warning and Opinion on Virtual Currencies // Central Bank of Ireland. [Электронный ресурс]. URL: <https://www.centralbank.ie/consumer-hub/consumer-notices/eba-opinion-on-virtual-currencies> (дата обращения: 02.02.2025).
3. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance) // *OJ L 150*, 9.6.2023, p. 40–205.

4. Authorisation of Issuers of Asset-Referenced Tokens and Electronic Money Tokens Guidance Note Under Regulation (EU) 2023/1114 (Markets in Crypto Assets Regulation) // Central bank of Ireland. URL: <https://www.centralbank.ie/docs/default-source/regulation/micar/guidance-note-for-the-issuers-of-arts-and-emts.pdf>.
5. MiCA's impact on USDT and the EU crypto landscape // The Block. [Электронный ресурс]. URL: <https://www.theblock.co/post/332613/micas-impact-on-usdt-and-the-eu-crypto-landscape> (дата обращения: 02.02.2025).
6. MiCA creates a new framework for crypto custody // The banker. [Электронный ресурс]. URL: <https://www.thebanker.com/content/65859bb9-d4e3-5532-9a34-7ca1b49e0b46> (дата обращения: 16.02.2025).
7. MiCA's impact on USDT and the EU crypto landscape // The Block. [Электронный ресурс]. URL: <https://www.theblock.co/post/332613/micas-impact-on-usdt-and-the-eu-crypto-landscape> (дата обращения: 02.02.2025).
8. The Impact of MiCA Laws on Europe's Cryptocurrency Landscape // MEXC. [Электронный ресурс]. URL: <https://blog.mexc.com/the-impact-of-mica-laws-on-europes-cryptocurrency-landscape-creator-mckingston/?ysclid=m6necr9usb361322409> (дата обращения: 02.02.2025).
9. Tether Removal Puts Europe at Risk of Missing Trump Crypto Boom // Bloomberg. [Электронный ресурс]. URL: <https://www.bloomberg.com/news/articles/2024-12-20/tether-mica-exit-puts-europe-at-risk-of-missing-crypto-boom-usdt> (дата обращения: 16.02.2025).
10. MiCA's impact on USDT and the EU crypto landscape // The Block. [Электронный ресурс]. URL: <https://www.theblock.co/post/332613/micas-impact-on-usdt-and-the-eu-crypto-landscape> (дата обращения: 02.02.2025).
11. MiCA Regulations and Their Impact on the Crypto Industry // Ulam Labs. URL: <https://www.ulam.io/blog/mica-regulations-and-their-impact-on-the-crypto-industry#Effect-on-Innovation-and-Startups-in-the-Crypto-Space> (дата обращения: 16.02.2025).
12. Ilya Kokorin, The anatomy of crypto failures and investor protection under MiCAR, Capital Markets Law Journal, Volume 18, Issue 4, November 2023. P 500–525.
13. EBA Warning and Opinion on Virtual Currencies // Central Bank of Ireland. [Электронный ресурс]. URL: <https://www.centralbank.ie/consumer-hub/consumer-notices/eba-opinion-on-virtual-currencies> (дата обращения: 02.02.2025).
14. MiCA: The good, the bad and the ugly of the EU's crypto rules // Cointelegraph. [Электронный ресурс]. URL: <https://cointelegraph.com/news/mica-good-bad-ugly-european-union-crypto-rules> (дата обращения: 02.02.2025).
15. Расследование преступлений, совершенных с использованием криптовалюты: Учебное пособие / Д. А. Иванов, М. М. Макаренко, В. В. Пушкарёв, Е. А. Русскевич. – Москва : Ай Пи Ар Медиа, 2021. – 80 с.
16. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

17. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

18. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

19. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

Гавирова Г. А.¹,
 курсант института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
 заместитель начальника кафедры
 противодействия преступлениям в сфере
 информационно-телекоммуникационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат юридических наук, доцент

МЕТОДЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Киберпреступность стала одной из главных угроз 21 века. В современных условиях стремительной цифровизации общества проблема киберпреступности приобретает глобальный характер, требующий комплексного подхода к ее решению. Киберпреступность представляет собой совокупность противоправных действий, совершаемых с использованием компьютерных технологий и сети Интернет, что существенно усложняет процесс их выявления и пресечения. При этом злоумышленники постоянно совершенствуют методы атак: от фишинга и спаминга до кибертерроризма. В таких условиях эффективное противодействие киберпреступности требует многоуровневого подхода, сочетающего технические инновации, правовое регулирование, повышение цифровой грамотности.

Объектом исследования являются общественные отношения в сфере противодействия киберпреступности.

Преступные деяния, осуществляемые злоумышленниками в информационном пространстве, относятся к довольно опасным и непредсказуемым, поскольку причиняют серьезный вред личности, обществу и государству. Делается вывод о том, что киберпреступления представляют угрозу не только для общественной, но и национальной безопасности России. Вопросы противодействия киберпреступлениям являются довольно актуальными не только в современной России, но и во всем мире. По оценкам Интерпола преступления, совершаемые в сети Интернет, считаются самыми краткими во всем мире. Общественно опасные деяния, осуществляемые виновными в информационном пространстве, относятся к самым внезапным и опасным, поскольку ущерб, причиненный такими видами посягательств, не имеет границ.

В условиях цифровой трансформации и роста онлайн-взаимодействия в РФ фиксируется расширение спектра киберугроз. Среди наиболее распространенных форм противоправных действий выделяются:

¹ © Гавирова Г. А., 2025.

1. Мошенничество через фишинговые ресурсы. Злоумышленники создают поддельные сайты, имитирующие официальные платформы банков, онлайн-магазинов для кражи персональных данных пользователей.

2. Несанкционированный доступ к информации. Включает в себя сбои в работе дистанционных образовательных платформ, например, срыв онлайн-занятий, а также взломы сайтов государственных органов, учреждений здравоохранения и социальных служб для незаконного получения служебных данных.

3. Киберсталкинг и незаконный оборот наркотических и психотропных веществ. Преследование в цифровом пространстве и распространение наркотических средств через зашифрованные каналы связи остаются значимыми проблемами.

Для снижения уровня цифровой преступности требуется комплексный подход, сочетающий технические, организационные и правовые механизмы. Рассмотрим некоторые меры противодействия киберпреступности.

Технологический аспект противодействия включает в себя разработку и внедрение специализированных программных и технических средств защиты. К ним относятся системы обнаружения вторжений (IDS/IPS), антивирусные программы нового поколения, межсетевые экраны, средства криптографической защиты информации и системы мониторинга сетевого трафика. Особое внимание уделяется развитию технологий искусственного интеллекта и машинного обучения для прогнозирования и предотвращения кибератак.

Организационные меры предполагают создание специализированных подразделений в правоохранительных органах, занимающихся расследованием киберпреступлений. В России функционируют отделы "К", которые специализируются на раскрытии преступлений в сфере информационных технологий. Важным элементом является также создание центров реагирования на компьютерные инциденты (CERT), которые обеспечивают оперативную реакцию на кибератаки и координацию действий различных организаций.

Международное сотрудничество играет ключевую роль в противодействии трансграничной киберпреступности. Создана система взаимодействия между правоохранительными органами разных стран, функционируют международные организации по борьбе с киберпреступностью. Особое значение имеет подписание международных соглашений о взаимной правовой помощи в расследовании киберпреступлений и экстрадиции преступников.

Профилактические меры направлены на предотвращение киберпреступлений и повышение осведомленности пользователей. К ним относятся:

- проведение обучающих мероприятий для различных категорий граждан;
- разработка методических рекомендаций по обеспечению информационной безопасности;
- создание специализированных образовательных программ;
- распространение информационных материалов о правилах безопасного поведения в сети.

Правовой аспект противодействия киберпреступности включает совершенствование законодательства в данной сфере. В Уголовном кодексе РФ предусмотрены специальные статьи, регламентирующие ответственность за преступления

в сфере компьютерной информации (гл. 28). Однако постоянное развитие технологий требует регулярного обновления нормативно-правовой базы. Актуальной задачей является корректировка ст. 272.1 УК РФ. Предлагается заменить формулировку «неправомерный доступ к охраняемой законом компьютерной информации» на «получение данных путем введения в заблуждение или методов социальной инженерии». Это уточнит квалификацию действий, связанных с обманом пользователей.

Технические методы защиты постоянно совершенствуются в ответ на появление новых видов кибератак. Современные системы защиты используют:

1. Многофакторную аутентификацию.
2. Биометрические системы идентификации.
3. Технологии блокчейн для защиты данных.

Человеческий фактор остается одним из наиболее уязвимых звеньев в системе информационной безопасности. Исследования показывают, что значительная часть кибератак удается благодаря социальной инженерии и манипулированию людьми. Поэтому важнейшим направлением является повышение кибергигиены населения и формирование культуры безопасного поведения в цифровом пространстве.

Институциональные меры предполагают создание эффективных механизмов координации между различными ведомствами и организациями. Формируются межведомственные рабочие группы, разрабатываются единые стандарты реагирования на киберугрозы, создаются системы обмена информацией между участниками процесса противодействия киберпреступности.

Существуют и экономические аспекты противодействия киберпреступности:

- финансирование разработки новых технологий защиты;
- инвестиции в подготовку специалистов;
- создание страховых механизмов для компенсации ущерба от кибератак;
- развитие рынка услуг по обеспечению информационной безопасности.

Образовательные программы играют ключевую роль в формировании кадрового потенциала для противодействия киберпреступности. Создаются специализированные кафедры в вузах, проводятся курсы повышения квалификации для сотрудников правоохранительных органов, разрабатываются программы профессиональной переподготовки.

Научно-исследовательская деятельность направлена на изучение новых видов киберугроз и разработку методов их нейтрализации. Проводятся исследования в области криптографии, компьютерной криминалистики, защиты от DDoS-атак, обнаружения вредоносного ПО.

Общественный контроль становится важным элементом системы противодействия киберпреступности. Формируются общественные организации, занимающиеся просвещением населения в сфере информационной безопасности, проводятся социальные кампании по повышению осведомленности граждан о киберугрозах.

Международные стандарты играют важную роль в унификации подходов к противодействию киберпреступности. Разрабатываются единые протоколы реагирования на киберугрозы, создаются международные базы данных о киберпреступлениях, формируются общие методики расследования.

Государственные меры противодействия киберпреступности включают в себя финансирование исследований в области кибербезопасности, разработка нормативно-правовой базы, международное сотрудничество в сфере кибербезопасности.

В заключение следует отметить, что эффективное противодействие киберпреступности возможно только при комплексном подходе, содержащем в себе постоянное совершенствование технических средств защиты, развитие нормативно-правовой базы, повышение квалификации специалистов, развитие международного сотрудничества, формирование культуры кибербезопасности в обществе. Только такой комплексный подход позволит обеспечить надежную защиту от киберугроз и эффективно противодействовать киберпреступности в современных условиях.

Список литературы

1. Голубев В. А. «Кибертерроризм» – миф или реальность? Центр исследования компьютерных преступлений / В. А. Голубев // Computer Crime Research Centre: [сайт]. – URL: <http://www.crime-research.org/> (дата обращения 11.05.2025).
2. Киберпреступность – определение, классификация киберпреступлений. – URL: <https://elcomrevue.ru/blog/cybercrime/kibeoprestupnost-chto-eto/> (дата обращения: 11.05.2025).
3. Романов, И. В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовнопроцессуальные и криминалистические чтения. – 2016. – № 5 (13). – С. 105–109.
4. Пракаш С. У. Новианди Нур П. Е. Анализ кибершпионажа в международном праве и индонезийском праве // Обзоры гуманитарных и социальных наук. 2019. Т. 7. № 3. С. 38–44.
5. Фурнелл С., Доулинг С. Киберпреступность: портрет ландшафта // Журнал криминологических исследований, политики и практики. 2019. Т. 5. № 1. С. 13–26.
6. Хрусталева Е. Ю. Костюрин Г. А. Киберугрозы: причины и рекомендации по предотвращению // Национальные интересы и безопасность. 2019. Т. 15. № 6 (375). С. 1185–1194. DOI: 10.24891/ni.15.6.1185.
7. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
8. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

9. Пушкарев, В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

10. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

11. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

12. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Гальцова С. А.¹,
 курсант института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
 заместитель начальника кафедры
 противодействия преступлениям
 в сфере информационно-телекоммуникационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат юридических наук, доцент

КИБЕРАТАКИ И ИХ ОБЩЕСТВЕННАЯ ОПАСНОСТЬ

Безусловно, на сегодняшний день с кибератаками знакомо большое количество людей не только в России, но и за рубежом. Если рассматривать статистику России, то за текущий период 2024 г. было зарегистрировано 765 тыс. преступлений, которые совершены с использованием информационно-телекоммуникационных технологий или, другими словами, с помощью компьютерной информации. Эта статистика показывает рост преступлений, а точнее на 13,1 % больше, чем за 2023 г.

Кибератаками называется способы получения несанкционированного доступа к конфиденциальным данным человека с задачей украсть, изменить, а в дальнейшем возможность уничтожения личных данных [1].

Также есть такое понятие, как кибербезопасность – это набор методов и способов защиты от атак злоумышленников для компьютерных сетей, мобильных устройств и иных данных. Это понятие раздел находит место во многих областях применения, как на работе, так и дома.

Кибербезопасность не ограничивается лишь техническими аспектами. Это комплексная проблема, требующая гармоничного взаимодействия технических мер безопасности. Такие атаки совершают как единичные злоумышленники, так и специально созданные организации, в которых есть заданные цели, мотивы, а также с умышленной формой вины.

Цифровые атаки – новая разновидность кибератак, представляет из себя объединение цифровых технологий и социальной инженерии. Такие атаки создают нападение не на программы, операционные системы или оборудование, а на психологию людей.

Предотвращение кражи или уничтожение информации является основной целью кибербезопасности. Рассмотрим виды киберугроз:

1. Киберпреступление.

¹ © Гальцова С. А., 2025.

2. Кибератака.
3. Кибертерроризм.

Проблемой общества на данном этапе развития считается кибератаки, которые приносят материальный ущерб компаниям, а также гражданам. В двадцать первом веке и злоумышленники пользуются многочисленным инструментарием, которыми пользуются при совершении атак. С каждым днем способы кибератак совершенствуются.

Чтобы завладеть доступом к персональным данным злоумышленники используют разные инструменты и приемы. Также в деятельности злоумышленников проявляются разные типы кибератак [2]:

1. Внедрение вредоносного программного обеспечения.
2. Эксплуатация уязвимостей автоматизированных систем.
3. Сканирование сетей.
4. Прослушивание (перехват) сетевого трафика.
5. Спуфинг.
6. Блокирование доступа или «отказ в обслуживании».
7. Социальная инженерия.

Теперь приходим к выводу, что важным понятием информационной безопасности является кибербезопасность информации. Ею называют уровень защищенности информации, при которой защищены основные принципы обеспечения кибербезопасности. В данные принципы входит: конфиденциальность, целостность, доступность.

Считается, что целенаправленные и отработанные кибератаки наносят больший имущественный вред. Примером кибератак служат истории о том, как компании взламывают и происходит утечка личных данных клиентов, в результате чего эту конфиденциальную информацию выкупают различные компании.

Для злоумышленников не имеет значение какой инфраструктурой пользуется его «жертва»- облачная или локальная. Важным для них является целостность передаваемой информации, которой необходимо завладеть. В таких действия можно выделить несколько видов кибератак:

1. Целевые кибератаки. Данные атаки имеют такое название из-за заранее планирования данного действия на конкретную «жертву». Выгода таких «нападений» заключается в том, что злоумышленник получает необходимую информацию, а также остается в сети до того момента пока его не раскроют. Для таких кибератак будет характерна долгая подготовка с определенным планом действия и инструментарием.

2. Распределенные кибератаки. Данные атаки осуществляются с помощью бот-сети и задействует большой круг «жертв», которых находят через утекшие базы взломанных ранее организаций.

При целевых атаках всегда есть возможность защититься. Для упрощения понятия условно делят на несколько этапов [3]:

- 1) противодействие на этапе подготовки кибератаки;
- 2) противодействие на этапе проникновения;
- 3) выявление на этапе закрепления в сети.

На первом этапе для специалистов информационной безопасности главной задачей стоит усложнение выявления уязвимых мест, с помощью которых в последствии можно атаковать.

На втором этапе сотрудники информационной безопасности должны следить за тем, как происходит взаимодействие компонентов защиты.

На третьем этапе сотрудники информационной безопасности контролируют отсутствие свободного доступа у работников. В данный этап будет входить выявление неких аномалий. Заключительным является уже реагирование на завершающих стадиях кибератаки, скорее всего атаку уже невозможно.

Общественная опасность кибератак заключается в разных последствиях для потерпевшего. Такими могут выступать потери денежных средств, утечка персональных данных, нарушение конфиденциальной информации, психологическое давление, а в некоторых случаях вред также может быть причинен и самому оборудованию.

Уголовное законодательство совершенствуется и не оставляет без внимания преступления в области компьютерной информации. Данным преступление в Уголовном кодексе Российской Федерации посвящена глава 28. В этой главе включены статьи с 272 по 274.2, которые часто редактируют. Также без внимания нельзя оставить разъяснения постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоение и растрате», в котором также толкуется преступления, связанные с кибератаками.

Но на данном этапе расследования преступления связанных с кибератаками поиски преступников затягиваются из-за отсутствия данных о местоположении, из-за использования различных программно-технических средств, позволяющих оставлять цифровые следы в Интернете.

Содействуют правоохранительным органам «белые хакеры», данное название носят специалисты в области кибербезопасности. Их работа заключается в тестировании ИТ-систем, совершая атаки для нахождения уязвимых точек. Главным различием от мошенников является то, что о найденных слабых местах «белые хакеры» сообщают владельцу, получая от него вознаграждение. В условиях санкций государственные системы нуждаются в нахождении всех слабых точек из-за агрессивного поведения недружественных стран.

В настоящее время ведется рассмотрение поправок в законодательство Российской Федерации для возможности проводить данные мероприятия по выявлению уязвимых точек с помощью привлечения иных специалистов. Усовершенствование законодательства исключат привлечение к уголовной ответственности за неправомерный доступ к компьютерной информации. Для работы таких специалистов необходимо официальное разрешение компании на свою деятельность.

Сотрудники ОВД совместно с иными специалистами в сфере информационной безопасности проводят кропотливую работу, для выявления лиц причастных к совершаемым преступлениям в информационной среде.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.04.2023). – Текст: электронный // КонсультантПлюс: [сайт]. – 2025. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ / (дата обращения: 07.05.2025).
2. Краткая характеристика состояния преступности в Российской Федерации за январь–март 2023 года. – Текст: электронный // Официальный сайт Министерства внутренних дел Российской Федерации: [сайт]. – 2025. – URL: <https://мвд.рф/reports/item/37377025/> (дата обращения: 07.05.2025).
3. Абдуллаев Э. А. Кибербезопасность: вызовы и стратегии защиты в цифровую эпоху / Э. А. Абдуллаев. – Текст: непосредственный // Молодой ученый. – 2023. – № 33 (480). – С. 8–9. – URL: <https://moluch.ru/archive/480/105493/> (дата обращения: 08.05.2025).
4. Аррыкова Гульджемал Керимназаровна, Аширов Илмырат Гелдимырадович, Язбердиева Айна Язбердиевна, Юзбашыева Джемиле Дурдымухаммедовна КИБЕРАТАКИ НА СЕТЕВЫЕ ПРОТОКОЛЫ: МЕТОДЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ // Наука и мировоззрение. 2025. № 39. URL: <https://cyberleninka.ru/article/n/kiberataki-na-setevye-protokoly-metody-obnaruzheniya-i-predotvrascheniya> (дата обращения: 09.05.2025).
5. Кодацкий Н. М., Мотуз А. С. Кибератаки анализ и риски // StudNet. 2022. №1. URL: <https://cyberleninka.ru/article/n/kiberataki-analiz-i-riski> (дата обращения: 08.05.2025).
6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
7. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
8. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
9. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
10. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.
11. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

12. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Галямина И. А.¹,
курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
заместитель начальника кафедры
противодействия преступлениям
в сфере информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

В последние годы наблюдается стремительный рост преступности в сфере информационных технологий. Киберпреступники становятся все более изощренными, используя различные методы для совершения своих преступлений, таких как фишинг, кража личных данных, DDoS-атаки, ransomware и другие. Это приводит к значительным финансовым потерям, а также к серьезным угрозам для безопасности и конфиденциальности данных жителей любой страны.

В настоящее время со стороны всех цивилизованных государств мира уделяется колоссальное внимание развитию информационных технологий и непосредственно ИИ, внедряя его достижения в самые различные сферы общественной жизни.

Так, Президент Российской Федерации В. В. Путин в выступлении на пленарном заседании Конференции по искусственному интеллекту «Путешествие в мир искусственного интеллекта», проходившей в Москве 11 декабря 2024 г., отметил особую значимость развития информационных технологий и подчеркнул, что ИИ обладает огромным потенциалом абсолютно в любых направлениях и отраслях человеческой жизнедеятельности [1].

Искусственный интеллект (ИИ) представляет собой набор технологий, которые позволяют компьютерам имитировать человеческий интеллект. ИИ обладает огромным потенциалом для борьбы с киберпреступностью [2]. Системы ИИ могут анализировать большие объемы данных, выявлять подозрительные действия, прогнозировать кибератаки и многое другое.

Целью данной статьи является анализ актуальных проблем использования технологий искусственного интеллекта в раскрытии и расследовании преступлений. В статье будут рассмотрены этические, технические и правовые проблемы,

¹ © Галямина И. А., 2025.

связанные с использованием искусственного интеллекта в правоохранительной деятельности.

В современных правоохранительных органах активно внедряются технологии искусственного интеллекта (ИИ), предоставляющие широкие возможности для повышения эффективности работы и более эффективного противодействия преступной деятельности [4].

Одной из ключевых областей применения ИИ является анализ данных. Системы мониторинга сетевой активности позволяют выявлять аномалии, такие как попытки несанкционированного доступа или аномальные транзакции, что способствует раннему обнаружению потенциальных преступлений. Помимо этого, системы анализа социальных сетей активно применяются для выявления потенциальных экстремистов или террористов среди пользователей сетей. Также важным инструментом являются системы прогнозирования, которые анализируют исторические данные и помогают определить вероятность совершения преступления, что облегчает превентивные меры правоохранительных органов.

Для противодействия кибератакам применяются алгоритмы машинного обучения. Они основаны на анализе поведения пользователей и выявлении аномалий, которые могут свидетельствовать о возможной кибератаке. Анализ уязвимостей позволяет выявить и устранить потенциальные уязвимости системы, а также прогнозировать их возможное использование злоумышленниками. Кроме того, системы анализа угроз активно отслеживают новые киберугрозы и разрабатывают методы их предотвращения.

Распознавание лиц и объектов также играет важную роль в деятельности правоохранительных органов. Технологии распознавания лиц используются для идентификации людей по фотографиям или видеозаписям, что может помочь в розыске преступников или поиск пропавших без вести лиц [5]. Распознавание объектов применяется для обнаружения идентификации предметов, таких как оружие, наркотики или взрывчатые вещества, что значительно облегчает расследование преступлений.

ИИ-чатботы становятся все более распространенным инструментом для поддержки сотрудников правоохранительных органов. Они автоматизируют рутинные задачи, предоставляют необходимую информацию и даже могут оказывать психологическую поддержку сотрудникам, что снижает их нагрузку и повышает эффективность работы [3].

Важно отметить, что использование ИИ в правоохранительной деятельности находится на ранней стадии развития. Несмотря на значительные преимущества, существуют этические, технические и правовые проблемы, которые требуют решения перед широким внедрением этих технологий в данной сфере.

Одна из основных проблем – этические вопросы. Алгоритмы ИИ могут проявлять предвзятость, что может привести к дискриминации определенных групп людей. Также они часто непрозрачны, затрудняя контроль и ответственность за ошибки. Использование ИИ может угрожать праву на частную жизнь, так как приводит к массовому сбору и анализу персональных данных.

Технические проблемы также играют важную роль. Не всегда можно полагаться на точность и надежность систем ИИ, что может привести к ошибкам в

расследовании преступлений. Кроме того, результаты работы систем могут быть сложными для интерпретации, что осложняет их использование в судебных процессах. Для работы с системами ИИ требуются высококвалифицированные кадры, которых может не хватать.

Правовые проблемы также необходимо учитывать. Неясно, насколько допустимо использовать данные, полученные с помощью ИИ, в качестве доказательств в суде [6]. Также не определено, кто несет ответственность за ошибки и сбои систем ИИ. Не существует достаточного правового регулирования использования ИИ в правоохранительной деятельности.

Эти проблемы представляют серьезные препятствия для широкого использования ИИ в правоохранительной деятельности. Решение этих проблем требует разработки этических принципов, повышения точности и надежности систем, обеспечения их прозрачности и подотчетности, подготовки квалифицированных кадров и разработки правового регулирования использования ИИ в данной сфере.

Помимо выявленных проблем, важно рассмотреть и перспективы дальнейшего развития искусственного интеллекта в борьбе с киберпреступностью. При этом необходимо обратить внимание на возможные пути решения описанных ранее проблем. Такой анализ позволит не только понять, какие новые возможности может предоставить использование ИИ, но и как эффективно преодолеть вызовы, стоящие перед его внедрением в правоохранительных органах.

В развитии борьбы с киберпреступностью с использованием искусственного интеллекта (ИИ) видится ряд перспектив, требующих системного подхода и участия различных сторон.

Прежде всего, совершенствование алгоритмов ИИ направлено на повышение их точности и надежности. Это включает разработку алгоритмов, способных обнаруживать более широкий спектр киберпреступлений, минимизировать ошибки и улучшать интерпретацию результатов.

Одновременно необходимо разработать новые этические нормы и стандарты использования ИИ. Эти принципы должны гарантировать справедливость, прозрачность, подотчетность и защиту частной жизни.

Важным аспектом является подготовка кадров для работы с системами ИИ. Это включает обучение сотрудников правоохранительных органов работе с такими системами, интерпретации их результатов и ознакомление с этическими принципами использования ИИ [3].

Для успешной реализации этих идей необходимо также сотрудничество между правоохранительными органами и разработчиками ИИ. Совместная работа позволит разработать более эффективные системы ИИ, решить этические проблемы и обеспечить правовое регулирование.

Важно отметить, что развитие ИИ имеет большой потенциал для борьбы с киберпреступностью, однако для его реализации необходимо решить ряд проблем. Совместные усилия правоохранительных органов, разработчиков ИИ и общества могут сделать искусственный интеллект мощным инструментом для обеспечения безопасности в киберпространстве.

Использование ИИ в раскрытии и расследовании преступлений имеет как преимущества, так и недостатки. С одной стороны, ИИ может помочь правоохранным органам быстрее и эффективнее расследовать преступления, предотвращать их совершение и обеспечивать безопасность. С другой стороны, его использование вызывает ряд этических, технических и правовых проблем, которые требуют комплексного подхода для решения.

Важно, чтобы развитие и использование ИИ в правоохранительной деятельности осуществлялись с соблюдением этических норм, научными методами и соответствовали правовым нормам. При грамотном подходе ИИ станет мощным инструментом для борьбы с киберпреступностью и обеспечения безопасности в обществе.

Список литературы

1. Конференция по искусственному интеллекту. Официальный сайт Президента России [Электронный ресурс]. – Режим доступа: URL: <http://www.kremlin.ru/events/president/news/62003> (дата обращения: 24.04.2025)/
2. Афанасьев А. Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Библиотека криминалиста. Научный журнал. 2018. № 3 (38). С. 28–34.
3. Конференция по искусственному интеллекту. Официальный сайт Президента России [Электронный ресурс]. – Режим доступа: URL: <http://www.kremlin.ru/events/president/news/62003> (дата обращения: 24.03.2025).
4. Кравцов Д.А. Искусственный разум: предупреждение и прогнозирование преступности. Вестник Московского университета МВД России. 2018;(3): 108–110.
5. МВД при помощи камер начнет искать преступников по татуировкам и походке. РБК // [Электронный ресурс]. – Режим доступа: URL: https://www.rbc.ru/technology_and_media/24/02/2020/5e4fb5af9a7947cfd5e1e3 (дата обращения: 24.03.2024).
6. Национальная стратегия развития искусственного интеллекта на период до 2030 года. Утв. Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». КонсультантПлюс [Электронный ресурс]. – Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 24.03.2025).
7. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
8. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

9. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
10. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
11. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
12. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
13. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарёв, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Горбачева А. А.¹,
курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Михайленко Н. В.,
доцент кафедры противодействия
преступлениям в сфере информационно-
телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ЭВОЛЮЦИЯ КИБЕРПРЕСТУПНОСТИ: ОТ ХАКИНГА ДО КРИПТОДЖЕКИНГА И DEERFAKE

Киберпреступность прошла впечатляющий путь развития от простых взломов компьютерных систем до сложных высокотехнологичных преступлений, использующих искусственный интеллект и машинное обучение. Эта эволюция отражает не только технологический прогресс, но и постоянно растущую изощренность методов преступной деятельности в цифровом пространстве.

Ранний этап киберпреступности характеризовался преимущественно хакерской активностью. Хакеры того времени действовали преимущественно из интереса к технологиям и желания проверить свои навыки. Их деятельность часто носила демонстративный характер и была направлена на доказательство возможности взлома систем. Основными методами были подбор паролей, использование уязвимостей программного обеспечения и социальная инженерия.

Следующий этап развития киберпреступности ознаменовался появлением организованной преступности в цифровом пространстве. Киберпреступники начали объединяться в группы, специализирующиеся на конкретных видах преступлений: фишинге, мошенничестве с банковскими картами, распространении вредоносного ПО. Появились первые ботнеты – сети зараженных компьютеров, используемых для рассылки спама и DDoS-атак.

Современный этап характеризуется появлением принципиально новых видов киберпреступлений. Одним из наиболее опасных направлений стал криптоджекинг – несанкционированное использование вычислительных ресурсов для майнинга криптовалют. Преступники внедряют вредоносное ПО в компьютеры пользователей или серверы организаций, заставляя их оборудование работать на добычу цифровых активов.

¹ © Горбачева А. А., 2025.

Технология deepfake представляет собой качественно новый уровень киберпреступлений. Используя алгоритмы машинного обучения и искусственный интеллект, злоумышленники создают поддельные аудио- и видеоматериалы, практически неотличимые от настоящих. Это открывает широкие возможности для шантажа, мошенничества и дискредитации личности.

Методы социальной инженерии постоянно совершенствуются. Киберпреступники используют психологические приемы и знания о поведении людей для получения конфиденциальной информации. Появились новые схемы обмана: от претекстинг-атак до сложных многоступенчатых мошеннических схем, включающих элементы социальной инженерии и технического взлома.

Кибершпионаж превратился в одно из самых опасных направлений киберпреступности. Государства и частные организации активно используют цифровые технологии для сбора конфиденциальной информации. Методы включают как классические взломы, так и использование сложных эксплойтов нулевого дня, а также компрометацию цепочек поставок программного обеспечения.

Финансовые преступления в цифровом пространстве достигли беспрецедентного уровня. Киберпреступники используют сложные схемы отмывания денег, манипулируют криптовалютными биржами, организуют схемы Ponzi и фишинг-атаки на финансовые учреждения. Появились новые виды мошенничества, связанные с ICO и DeFi-проектами.

Кибертерроризм представляет собой особую угрозу. Злоумышленники нацелены на нарушение работы критически важной инфраструктуры: энергетических систем, транспортных узлов, систем водоснабжения и здравоохранения. Используются методы DDoS-атак, внедрения вредоносного ПО и компрометации систем управления.

Кибербуллинг и онлайн-травля эволюционировали в сложные схемы психологического давления и манипуляции. Злоумышленники используют социальные сети, мессенджеры и другие платформы для распространения дезинформации, шантажа и травли жертв. Появились новые формы кибербуллинга, включая создание поддельных аккаунтов и распространение компромата.

Защита от киберпреступлений требует комплексного подхода. Современные системы безопасности включают:

1. Многофакторную аутентификацию.
2. Системы обнаружения вторжений.
3. Технологии машинного обучения для выявления аномалий.
4. Криптографические методы защиты.
5. Системы резервного копирования.
6. Технологии блокчейн для защиты данных.

Профилактика киберпреступлений включает:

1. Повышение цифровой грамотности населения.
2. Разработку образовательных программ.
3. Создание специализированных центров реагирования.
4. Развитие международного сотрудничества.
5. Формирование единых стандартов безопасности.
6. Создание механизмов быстрого реагирования на инциденты.

Законодательное регулирование постоянно совершенствуется для борьбы с новыми видами киберпреступлений. Вводятся новые статьи уголовного кодекса, ужесточаются наказания, разрабатываются механизмы международного сотрудничества в расследовании преступлений. Особое внимание уделяется защите персональных данных и противодействию кибербуллингу.

Международное сотрудничество становится ключевым фактором в борьбе с киберпреступностью. Создаются специализированные организации, разрабатываются единые стандарты расследования, формируются механизмы обмена информацией между правоохранительными органами разных стран. Особое значение приобретает борьба с трансграничными преступлениями.

Технологические инновации в сфере кибербезопасности развиваются в нескольких направлениях:

1. Квантовые технологии шифрования.
2. Искусственный интеллект в системах обнаружения угроз.
3. Машинное обучение для прогнозирования атак.
4. Нейросетевые технологии в кибербезопасности.
5. Блокчейн-решения для защиты данных.

Человеческий фактор остается одним из наиболее уязвимых звеньев в системе кибербезопасности. Киберпреступники активно используют методы социальной инженерии, манипулирования и психологического давления. Поэтому важнейшим направлением остается повышение осведомленности пользователей и формирование культуры безопасного поведения в цифровом пространстве.

В заключение следует отметить, что эволюция киберпреступности отражает общий технологический прогресс и развитие общества.

Список литературы

1. Алексеев И. С. Расследование киберпреступлений: учебное пособие. – М.: Юнити-Дана, 2018.
2. Белов Е. Б., Романец Ю. В., Тимофеев П. В. Информационная безопасность и защита информации. Практикум. – М.: Горячая линия-Телеком, 2012.
3. Волеводз А. Г. Международное уголовное право: противодействие киберпреступности. – М.: Проспект, 2018.
4. Гаврилов Д. В. Киберпреступность: понятие, виды, способы совершения и предупреждения. – М.: ЮрИнфоР, 2017.
5. Ярочкин В. И. Информационная безопасность: учебник для студентов вузов. – М.: Академия, 2000.
6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
7. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

8. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
9. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
10. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35-37. – EDN HPTYOY.
11. Константинов А. В. Перспективы развития и использования искусственного интеллекта в целях противодействия преступлениям в сфере информационно-телекоммуникационных технологий / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов, Москва, 30 марта 2023 года / сост. А.В. Константинов. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 80–82.
12. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
13. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Гусева Е. В.¹,
 курсант института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
 заместитель начальника кафедры
 противодействия преступлениям
 в сфере информационно-телекоммуникационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат юридических наук, доцент

ПРОИЗВОДСТВО СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С ПРИМЕНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

На данный момент экспертами ведется дискуссия, связанная с внедрением технологий искусственного интеллекта. 13 марта 2022 г. в Москве была организована дискуссионная площадка IV Заседания Международного полицейского клуба на конференции «Права человека в цифровую эпоху». Ведущей темой дискуссии стал вопрос перехода на электронный формат уголовных дел, возможность внедрения новых автоматизированных систем в практическую деятельность органов государственной власти, вопросы нормативной регламентации.

Прийти к однозначному мнению о том, стоит ли в ускоренном порядке апробировать цифровые технологии, так и не удалось. Одни считают, что переход на новый формат позволит упростить процесс, связанный с уголовным производством. Другие же, отмечают возможность хакерских атак на информационные базы, а также утечку персональных данных [1].

Помимо этого, появляются новые серверы, способные оказывать содействие в раскрытии и расследовании преступлений, а также способствующие упрощению процесса поиска и сбора информации, которые также применяются в ходе производства сотрудниками органов предварительного расследования следственных действий.

Ввиду того, что технологии искусственного интеллекта относятся к категории информационных технологий, целесообразно рассмотреть теоретическую основу правовой регламентации цифровых технологий. Основу правовой регламентации применения информационных технологий составляют следующие нормативно-правовые акты: Конституция Российской Федерации – основной документ, гарантирующий права и свободы человека и гражданина. В частности, статья 23 предусматривает гарантию каждому на неприкосновенность частной

¹ © Гусева Е. В., 2025.

жизни, личную и семейную тайну; Уголовно-процессуальный кодекс Российской Федерации. Порядок работы с электронными носителями информации и (или) доказательствами регламентирован в УПК РФ. В частности, понятие «электронные носители информации» упомянуто в ряде статей (в некоторых случаях также со знаком «.1», что свидетельствует о реакции законодателя на современные условия путем своевременного изменения и дополнения федерального законодательства); государственные программные документы, определяющие общие направления развития информационных технологий в различных сферах общественной жизни и деятельности органов государственной власти. (Например, Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”, “Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года”»).

Реализация программы «Информационное общество» нацелена прежде всего на повешения качества жизни граждан, повышение для каждого гражданина возможности доступа к информационным технологиям, а также совершенствование законодательной базы, регламентации отношений, связанных с применением информационных технологий.

Стратегия развития отрасли информационных технологий имеет цель в определении комплексного и единого подхода государства в развитии информационных технологий. Приоритетные задачи в области развития информационных технологий: развитие информационно-телекоммуникационной сети «Интернет», повсеместное внедрение и усовершенствование; модернизация систем электронного документооборота; создание и развитие центров обработки данных внутри страны (минимизация фактора несанкционированного вмешательства зарубежных стран, осуществляемого с целью хищения персональных данных)

Нормативный правовой акт, содержащий основные понятие «информации» и «информационные технологии» – это Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 Федерального закона содержит основные понятия, информация – это определенные сведения, независимые от формы представления, информационные технологии – это совокупность процессов, методов поиска, хранения и обработки различных сведений [2].

В судебной системе одним из нормативных правовых актов, определяющим в качестве одного из направлений – применение информационных технологий, является Федеральная целевая программа «Развитие судебной системы России на 2013–2024 годы».

Одним из примером, иллюстрирующих возможность применения в ходе проведения следственного действия информационных технологий, является возможность использования средств фотографирования, аудио- и (или) видеозаписи, кино съемки. Данное действие регламентировано нормами уголовно-процессуального законодательства.

Однако в нормах уголовно-процессуального закона не конкретизировано положение о том, что техническое средство может применяться и защитником в ходе проведения следственного действия.

При проведении очных ставок адвокат Б. осуществлял аудиозапись, несмотря на возражения следователя. Действия адвоката были расценены следствием как нарушение ст. 4, п. 2 ст. 8, ч. 1 ст. 12 Кодекса профессиональной этики адвоката. В представлении было указано на нарушение нормы ч. 6 ст. 164 и ч. 4 ст. 189 УПК РФ, в которой указывается, что следователь в ходе проведения следственного действия разрешать иным лицам использовать технические средства.

Совет Адвокатской палаты в ходе рассмотрения материалов представления пришел к выводу о том, что применение адвокатом в ходе производства следственного действия средств технической фиксации базируется на конституционной гарантии защиты свои прав и свобод всеми возможными средствами, не противоречащими нормам закона [3].

В Федеральном законе № 3 «О полиции» от 7 февраля 2011 года отражено, что в процессе осуществления деятельности сотрудники полиции обязаны использовать достижения науки и техники, современных технологий и информационных систем. Можно констатировать, что применение информационных технологий является не только правом сотрудников органов внутренних дел, а обязанностью.

Использование электронных средств фиксации осуществляется с целью сбора доказательственной базы: оформление процессуальных документов, использование техники в качестве средства фиксации при производстве следственных действий (например, осуществление видеозаписи в ходе осмотра места происшествия), составление субъективного портрета лица (на основе показаний потерпевшего составляется фоторобот лица, подозреваемого в совершении преступления).

В настоящее время разрабатываются проекты, которые способны оказать воздействие в деятельности органов предварительного расследования. Учеными из Нижегородского университета имени Н.И. Лобачевского разрабатывается система «ФОРВЕР», позволяющая генерировать наиболее перспективные версии о личности преступника. Помимо этого, Министерством внутренних дел Российской Федерации был заключен контракт, согласно которому к концу 2023 г. в ведомстве будет использоваться специальная программа «Зеркало», позволяющая выявить монтаж, осуществленный посредством использования нейросети [4].

В деятельности органов предварительного расследования была попытка апробации специально разработанного комплекса «Автоматизированное рабочее место следователя (дознателя)» (АРМ). Основные задачи системы заключаются в следующем: Автоматизация документооборота; создание сетевых графиков расследования; анализ судебной практики по уголовным делам; разработка алгоритмов и рекомендаций, по дальнейшему расследованию преступлений; сопоставление и получении информации, которая является необходимой при всестороннем рассмотрении событий, относящихся к расследованию уголовного дела [5].

Было проведено большое количество исследований, рассматривающих эффективность применения АРМ в профессиональной деятельности органов предварительного расследования. Как отмечает Загвоздкин Н. Н. применение АРМ на практике не позволяет судить об эффективности прикладного сервиса, оказывающего содействие в осуществлении деятельности. В ходе апробации выявлен ряд недостатков, главный из которых – это отсутствие отдаленного доступа к информационным базам [6].

Переход на электронный формат ведения уголовных дел является одним из дискуссионных вопросов в настоящее время. 13 марта 2022 г. в Москве была организована дискуссионная площадка IV Заседания Международного полицейского клуба на конференции «Права человека в цифровую эпоху». Ведущей темой дискуссии стал вопрос перехода на электронный формат уголовных дел, мнения по данному вопросу разделились. Так, одни считают, что переход на новый формат позволит упростить процесс, связанный с уголовным производством. Другие же, отмечают возможность хакерских атак на информационные базы, а также утечку персональных данных.

Помимо этого, в Российской Федерации применяются справочно-правовые системы «КонсультантПлюс», «ГАРАНТ». Их использование помогает существенно упростить поиск необходимой информации.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) (электронный ресурс) // URL: https://www.consultant.ru/document/cons_doc_LAW_28399/?ysclid=lbe8c6zdus350028647.
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (электронный ресурс) // URL: http://www.consultant.ru/document/cons_doc_LAW_34481/.
3. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» [Электронный ресурс] // URL: https://www.consultant.ru/document/cons_doc_LAW_110165/73f31e44672736d57e7b4937fc7b72e270da480f/?hl=ru_RU&ysclid=lbjtzv8k6y834466936.
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (электронный ресурс) // URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/.
5. Загвоздкин Н. Н. Автоматизированное рабочее место следователя: проблемы разработки и внедрения в практику // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 1 (9). URL: <https://cyberleninka.ru/article/n/avtomatizirovannoe-rabochee-mesto-sledovatelya-problemy-razrabotki-i-vnedreniya-v-praktiku>.
6. Зайцев О. А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // Журнал зарубежного законодательства и сравнительного

правоведения. 2019. № 4. URL: <https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-elektronnoy-informatsii-v-kachestve-dokazatelstv-po-ugolovnomu-delu-sravnitelno-pravovoy-analiz>.

7. Цифровизация российского уголовного судопроизводства должна быть поэтапной (электронный ресурс) // URL: <https://www.advgazeta.ru/novosti/tsifrovizatsiya-rossiyskogo-ugolovnogo-sudoproizvodstva-dolzhna-byt-poetapnoy/>.

8. Пандемия как стимул развития онлайн-правосудия (электронный ресурс) // URL: <https://www.advgazeta.ru/mneniya/pandemiya-kak-stimul-razvitiya-onlayn-pravosudiya/?ysclid=lb9olohnl153543339>.

9. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

10. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

11. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

12. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

13. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

14. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарёв, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Дранникова Е. О.¹,

курсант института подготовки сотрудников

для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Михайленко Н. В.,

доцент кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета

МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В КИБЕРПРОСТРАНСТВЕ: АНАЛИЗ МЕТОДОВ, УЯЗВИМОСТЕЙ И МЕР ПРОТИВОДЕЙСТВИЯ

Социальная инженерия (СИ) стала одним из ключевых инструментов киберпреступников. По данным аналитиков, до 90 % всех взломов осуществляются с использованием человеческого фактора. Преступники все чаще выбирают обман и психологическое давление, а не дорогостоящие технические методы. Данная статья направлена на анализ методов социальной инженерии, выявление существующих уязвимостей и предложение мер противодействия с учетом правовых аспектов расследования таких преступлений.

Ежегодно растет количество преступлений, совершаемых с помощью цифровых технологий. По оценкам экспертов, до 98 % кибератак основываются на социальной инженерии. Интернет-аферисты активно используют обман и психологическое давление на людей, поэтому применение ими методов социальной инженерии признается одной из самых опасных угроз для государства, бизнеса и граждан. Особенно актуальна эта проблема для сотрудников органов внутренних дел, призванных осуществлять противодействие данным преступлениям.

Социальная инженерия (СИ) – это совокупность психологических приемов, позволяющих злоумышленникам получить у жертвы конфиденциальную информацию (пароли, данные карт, доступ к системам) или убедить ее совершить выгодные преступнику действия. Явление зародилось задолго до появления интернета, но в цифровую эпоху получило новую масштабность: электронная почта, соцсети, мессенджеры дают мошенникам почти неограниченный охват.

Несмотря на технический прогресс, основной целью атак по-прежнему является человек, обладающий психологическими уязвимостями, такими как доверчивость, страх, уважение к авторитету, любопытство и жадность. Используя эти слабости, злоумышленники добиваются от жертв необходимых действий или информации.

¹ © Дранникова Е. О., 2025.

Основными методами социальной инженерии являются: фишинг, вишинг, смишинг, претекстинг, байтинг, deepfake и ИИ-технологии [1, с. 50–54].

Одним из распространенных методов является фишинг, когда злоумышленники массово рассылают электронные письма с вредоносными ссылками, имитирующие официальные сообщения от банков или других авторитетных организаций. Телефонные мошенничества (вишинг) представляют собой звонки от якобы сотрудников банков или правоохранительных органов с требованием передать конфиденциальные данные. Также распространен смишинг – рассылка мошеннических сообщений через SMS и мессенджеры с просьбой перейти по ссылке или перезвонить по указанному номеру. Претекстинг – еще один метод, предполагающий создание злоумышленником детально проработанной легенды для убеждения жертвы в правдоподобности своих намерений. Байтинг (приманка) – использование физической или цифровой наживки, основанной на любопытстве или жадности жертвы. Новейшим методом становится использование технологий deepfake, позволяющих мошенникам создавать поддельные аудио- и видеоматериалы с участием реальных людей. Злоумышленники могут создавать «виртуальные звонки» от руководства и обманом получать доступ к финансам [2].

Успешности атак злоумышленников способствуют различные уязвимости.

Человеческий фактор остается ключевой уязвимостью, так как сотрудники организаций и обычные граждане зачастую не владеют необходимыми знаниями в области кибербезопасности и легко поддаются психологическим манипуляциям. Организационные недостатки, такие как отсутствие четких регламентов и инструкций по информационной безопасности, отсутствие регулярного обучения персонала и слабая культура безопасности также способствуют успешности атак. Технические уязвимости, включая использование устаревшего программного обеспечения, отсутствие антивирусов, фильтров электронной почты и многофакторной аутентификации, значительно облегчают задачу мошенникам. Кроме того, избыточная информационная открытость в социальных сетях и базах данных упрощает процесс подготовки злоумышленников к совершению атак.

Эффективное противодействие социальной инженерии требует комплексного подхода. Важнейшей мерой являются регулярное обучение и повышение осведомленности сотрудников и граждан о новых методах мошенничества, способах их распознавания и реагирования на попытки обмана. Для этого можно использовать регулярные тренинги, тестирование персонала, фишинг-симуляции. В организациях необходимо внедрять строгие политики безопасности, регламентирующие поведение сотрудников при обработке конфиденциальных данных и проведении финансовых операций. Технические меры включают использование актуальных антивирусных программ, фильтров для электронной почты, систем мониторинга и многофакторной аутентификации.

Формирование культуры информационной безопасности, где сотрудники чувствуют личную ответственность и проявляют бдительность, является не менее важным элементом противодействия.

Международное сотрудничество правоохранительных органов, обмен опытом и информацией о новых схемах мошенничества также играют важную роль в противодействии киберугрозам.

Преступления, связанные с киберпреступностью, сложны в расследовании, а правоохранительные органы нуждаются в кадрах с достаточно интеллектуальным потенциалом в сфере компьютерных технологий [3, с. 133–138]. В российском законодательстве социальная инженерия прямо не выделяется как отдельный состав преступления, однако такие деяния квалифицируются по общим статьям Уголовного кодекса Российской Федерации. Чаще всего действия социальных инженеров подпадают под мошенничество (статья 159 УК РФ), неправомерный доступ к компьютерной информации (статья 272 УК РФ), создание и распространение вредоносных программ (статья 273 УК РФ) и нарушения тайны личной жизни и связи (статьи 137, 138 УК РФ) [4]. При незначительном ущербе предусмотрена административная ответственность в соответствии с Кодексом РФ об административных правонарушениях (статья 7.27) [5]. Расследование таких преступлений требует оперативного взаимодействия с банковскими учреждениями, операторами связи и интернет-провайдерами, а также обязательного назначения компьютерно-технических и иных судебных экспертиз для сбора доказательной базы.

В последние годы все большую угрозу представляют атаки с использованием искусственного интеллекта (ИИ), такие как генерация реалистичных дипфейков и автоматическое создание убедительных фишинговых писем. Судебная практика по делам, связанным с социальной инженерией, свидетельствует о постепенном ужесточении наказаний, включая реальные сроки лишения свободы. Законодательство продолжает совершенствоваться, вводятся новые нормы, регулирующие ответственность за незаконное обращение персональных данных и противодействие киберугрозам. Для сотрудников МВД России важно своевременно реагировать на такие угрозы, совершенствовать знания и навыки работы с цифровыми доказательствами, активно взаимодействовать с коллегами из других ведомств и зарубежными партнерами. Поскольку социальная инженерия – преступление без границ, нужно стремиться к созданию всеобъемлющей системы международного противодействия [6, с. 678–695].

Борьба с социальной инженерией требует комплексных усилий. Необходимо совмещать правовые меры (неотвратимость наказания для кибермошенников), техническое укрепление систем, и главное – развитие человеческого «иммунитета» к обману. Сотрудники МВД России должны выступать не только как «карающий меч», но и как просветители и советники для населения. Разрабатывая профилактические программы, выступая в СМИ, взаимодействуя с образовательными организациями, полиция может существенно снизить число потенциальных жертв, научив граждан базовым правилам цифровой гигиены.

Таким образом, эффективная борьба с социальной инженерией требует от сотрудников правоохранительных органов высокого уровня подготовки, постоянного обучения и развития технических компетенций. Важным аспектом является также профилактическая работа с населением и организациями для минимиза-

ции рисков таких атак. Совершенствование законодательства и укрепление международного сотрудничества позволит существенно повысить уровень безопасности в киберпространстве.

Список литературы

1. Мельников А. И. Социальная инженерия в цифровой эпохе: анализ методов манипуляции человеческим фактором в целях кибератак // Социально-гуманитарные знания. 2024. №1. С. 50–54.
2. Данные компании Group-IB о мошеннических кол-центрах и deepfake, отчет 2024.
3. Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. 2021. № 1 (42). С. 133–138.
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».
5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 01.04.2025) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».
6. Клевцов К. К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам // Вестник СПбГУ. Серия 14. Право. 2022. № 3. С. 678–695.
7. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
8. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
9. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
10. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
11. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.

12. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

13. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарёв, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Егорова В. С.¹,

*курсант института подготовки сотрудников для органов
предварительного расследования Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Токолов А. В.,

*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ИСПОЛЬЗОВАНИЕ МЕССЕНДЖЕРОВ КАК СРЕДСТВО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

В 1961 году в Массачусетском Технологическом Институте в США была создана операционная система, позволяющая входить в информационную среду и обмениваться сообщениями до тридцати пользователей одновременно. Данное событие послужило началом эволюции материальных писем в электронную сеть. Первым мессенджером, набравшим популярность как в России, так и зарубежом является ICQ, созданный в 1996 году израильской компанией Mirabilis и принадлежащий на данный момент российской технологической компании Mail.ru Group. Это приложение уже в те года позволяло находить людей по базе пользователей, обмениваться с ними сообщениями и файлами, а также создавать многопользовательские чаты [1].

К настоящему времени среди населения Российской Федерации наиболее популярными являются мессенджеры WhatsApp, Telegram и Вконтакте. Они используются для общения между людьми, а также предоставляют возможность создания масштабных чатов для большого количества участников, групповые видеозвонки и др. С момента развития преступного мира в информационно-телекоммуникационных сетях, во многих мессенджерах была введена функция двухфакторной аутентификации, что является дополнительным уровнем безопасности для учетной записи, когда доступ к своему аккаунту может быть только у собственника странички, даже несмотря на то, что пароль от нее стал доступен злоумышленнику. Несмотря на сложность процедуры, взломать аккаунт все-таки возможно. Спектр преступлений в таком случае может быть различным.

Самым популярным способом совершения киберпреступления с использованием мессенджеров является массовая рассылка, содержащая ложные сведения или же ссылку, нажав на которую ни о чем не подозревающее лицо может раскрыть злоумышленнику свои личные данные, открыть доступ к аккаунту или сетевому соединению в целом [2]. Самым простым способом традиционно считается «выманивание» преступником денежных средств с помощью доверчивых

¹ © Егорова В. С., 2025.

друзей и родных жертвы, когда правонарушитель делает общую рассылку контактам потерпевшего сообщения следующего содержания: «Привет! Я попал в передрагу и у меня совсем не осталось денег на карте, ты не мог бы скинуть мне ... рублей? Верну тебе завтра или когда увидимся». Несмотря на малую затратность времени и средств для совершения представленного преступления, многие люди «ведутся» на них и действительно отправляют денежные средства, хотя очень часто злоумышленник, при попытке совершения данного общественно-опасного деяния, допускает некоторые ошибки, такие как:

1. Обращается к человеку, записанному в телефоне жертвы в формальном ключе с помощью неформального приветствия, что сразу же вызывает подозрения.

2. Ничего не объясняет, не пытается придумать причину, по которой ему необходима денежная сумма именно сейчас, в определенный момент.

3. Использует шаблон определенного сообщения и применяет его ко всему разностороннему кругу лиц в контактах потерпевшего, что определенно вызывает сомнения.

Несмотря на достаточно простую практику совершения преступлений при помощи общедоступных мессенджеров, бывают и более сложные мошеннические схемы. Например, когда преступник предлагает пользователю вложиться в криптовалюту через различные боты, которые в итоге оказываются частью мошеннической схемы и написаны злоумышленниками, вследствие чего вложенные средства машинально направляются на скрытый счет мошенника. Среди таких все наиболее популярными становятся боты социальной сети «Telegram», основанной в 2013 году. При помощи создания аккаунта с каким-либо официальным названием, к примеру, притворяясь «техподдержкой» Telegram, злоумышленники делают рассылку на различные аккаунты пользователей с предупреждением о том, что их аккаунт пытаются взломать. Стоит отметить, что такие сообщения содержат достаточно формализованный шаблон, известный каждому человеку, которого хотя бы раз пытались взломать или который менял когда-либо пароль к своему аккаунту. Только перейдя в профиль «техподдержки», можно увидеть, что это самый обычный аккаунт со скрытым номером. При этом данная деятельность выглядит достаточно подготовленно и качественно, речь настоящей поддержки по работе с пользователями копируется дословно и поэтому чаще всего не вызывает подозрения у обывателей. Для того, чтобы подобную схему мошенничества было тяжелее доказать, злоумышленники используют так называемый «секретный» чат, распознать который возможно по значку замка вверху имени пользователя. Такой вид чата не позволяет делать скриншот диалога, но если пользователь все-таки попытается сделать его, то вся предыдущая переписка будет стерта, и на фотографии вы сможете увидеть лишь пустое диалоговое окно.

Особенно тяжело раскрыть преступления с использованием нейросети, когда преступник посредством программы создает провокационное фото жертвы, не существовавшее в действительности, но настолько реальное, что потерпевший подвергается шантажу и даже выполняет требования преступника, боясь обра-

тяться в правоохранительные органы по личным соображениям. Сергей Полунин, руководитель группы защиты инфраструктурных ИТ компании «Газинформсервис», заявил: «Как правило, основные схемы мошенничества в мессенджерах – это фишинг разных видов. И необычность обычно заключается в том, какие истории придумывают злоумышленники, чтобы усыпить внимание потенциальных жертв. Классические заходы вроде сообщения от близкого человека, который оказался в беде или информации от банка о подозрительных действиях, не уходят в прошлое. Однако встречаются и куда более креативные подходы, включающие создание целых многоходовых историй, нацеленных на конкретного человека. При этом такой атаке предшествует разведка – чем человек интересуется, какие сайты посещает и с кем общается» [3].

Дипфейк-технологии, которые сочетают глубокое обучение и создание фейковых материалов, стали серьезной проблемой в нашем современном информационном обществе. Они не только используются в политических играх и мести, но и стали инструментом для шантажа и проведения масштабных мошеннических схем. Авторы дипфейков могут создать фейковое видео, которое кажется настоящим. Руководители крупных компаний могут оказаться под угрозой, когда мошенники угрожают опубликовать компрометирующие видео, способные серьезно подорвать их репутацию. В таких случаях, заплатив отступные, они пытаются предотвратить публикацию фейкового материала. Кроме того, мошенники могут использовать дипфейки в сочетании с социальной инженерией, чтобы получить доступ к конфиденциальной информации. Проникнув в сеть компании, выдавая себя за высокопоставленных сотрудников, обманом они способны заставить персонал предоставить им необходимые пароли и привилегии доступа. После этого, хакеры получают полный доступ к конфиденциальным данным, что может привести к серьезным последствиям для компании. В свете этих угроз важно принять меры для защиты от дипфейков и мошенничества. Компании должны обучать своих сотрудников основам безопасности, чтобы они могли распознавать подозрительные ситуации и быть более бдительными. Также необходимо использовать современные технологии и программное обеспечение для обнаружения дипфейков и предотвращения несанкционированного доступа к информации. Подытожив вышесказанное, отметим, что дипфейк-технологии представляют серьезную угрозу для компаний и частных лиц. Шантаж, мошенничество и нарушение конфиденциальности стали распространенными приемами, используемыми мошенниками. Однако, с повышенной осведомленностью и применением соответствующих мер предосторожности, мы можем снизить риски и защитить себя от этих угроз.

Важно подчеркнуть, что все больших масштабов достигает проблема распространения с помощью глобальной сети порнографических материалов несовершеннолетних. Так, в 2021 году был вынесен обвинительный приговор в отношении Д. С. Прошина, осуществивший приобретение с дальнейшим распространением материалов порнографического содержания с участием несовершеннолетних лиц. Из материалов судебной практики следует: «Д. С. Прошин, находясь по месту своего жительства и регистрации, используя личный мобильный телефон марки «Honor 9», позволяющий осуществлять выход в ИТКС

«Интернет», и осуществляя через данный мобильный телефон вход в вышеуказанный интернет-канал мессенджера «Telegram», действуя умышленно, осознавая общественную опасность и противоправный характер своих действий, игнорируя нормы общественной морали и нравственности, предоставил в вышеуказанном мессенджере созданную вышеописанным способом интернет-ссылку на хранящиеся в вышеуказанном облачном хранилище материалы с порнографическими изображениями несовершеннолетних лиц, которые согласно экспертным заключениям, являются материалами, содержащими порнографические изображения несовершеннолетних лиц, в том числе не достигших четырнадцатилетнего возраста. Доступ к вышеуказанной интернет-ссылке Прошиным Д. С. был предоставлен не известным ему пользователям мессенджера «Telegram» и Интернет-сайта «Mail.ru», таким образом он совершил приобретение, хранение в целях распространения, распространение материалов с порнографическими изображениями несовершеннолетних, совершенные с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть Интернет), т. е. совершил преступление, предусмотренное п. «г» ч. 2 ст. 242.1 УК РФ» [4].

Таким образом, человеку, использующему мессенджеры для простого общения или же ведения бизнеса, работы, стоит учитывать то, что информационная сеть – это лабиринт. То, что попадает в сеть, становится «иголкой в стоге сена» и уже никогда не будет удалено. Поэтому каждый раз, создавая пароль или набирая сообщение, стоит помнить о том, что нужно категорически исключить использование конфиденциальных данных и личной тайны, а также необходимо всегда задумываться, кому и что направлять; точно ли человек по ту сторону экрана является тем, кому вы желаете передать информацию.

Список литературы

1. Мессенджеры в России – больше, чем сервис для обмена сообщениями. Пример Telegram.». // Management interculturel et international [Электронный ресурс] URL: https://master-m2i.parisnanterre.fr/wp-content/uploads/2020/12/memoire-nabiullina-Adelya_Telegram.pdf (дата обращения: 20.04.2025).
2. Тертычная И. В., Бадзгарадзе Т. А., Проурзина О. Ю. Особенности выявления, раскрытия и расследования преступлений в сфере незаконного оборота наркотических веществ, совершенных с использованием информационно-коммуникационной сети «Интернет» // Аграрное и земельное право. 2022. № 9 (213) [Электронный ресурс] URL: <https://cyberleninka.ru/article/n/osobennosti-vyyavleniya-raskrytiya-i-rassledovaniya-prestupleniy-v-sfere-nezakonnogo-oborota-narkoticheskikh-veschestv-sovershennykh> (дата обращения: 20.04.2025).
3. Фишинг и чат-боты: как обезопасить себя в мессенджерах? // Cyber Media [Электронный ресурс] URL: <https://securitymedia.org/info/fishing-i-chat-boty-kak-obezopasit-sebya-v-messendzherakh.html> (дата обращения: 20.04.2025).
4. Приговор Раменского городского суда Московской области от 16.08.2021 года по делу № 1-498/2021// [Электронный ресурс] <https://судебныерешения.рф/62368204/extended#decision> (дата обращения: 20.04.2025).

5. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWQVQF.
6. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
7. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
8. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
9. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
10. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
11. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарёв, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Еремина А. А.¹,
курсант институт подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Старых С. М.,
доцент кафедры уголовного права
Московского университета
МВД России имени В.Я. Кикотя

НЕПРАВОМЕРНЫЙ ДОСТУП И НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: АНАЛИЗ И СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА УГОЛОВНО-ПРАВОВЫХ СОСТАВОВ

Общественноопасные деяния, совершаемые в сфере компьютерной информации, в настоящее время, представляют собой довольно серьезную проблему, как для правоохранительных органов, так и для простых граждан. Актуальность этой проблематики подтверждается тем, что как в нашей стране, так и за ее пределами практически все сферы жизнедеятельности в той или иной форме связаны с телекоммуникационной средой. Например, с банковской деятельностью, при осуществлении банковских операций, в области социальных услуг (предоставление услуг с помощью информационно-телекоммуникационной сети Интернет), при осуществлении государственного контроля за соблюдением гражданами законов Российской Федерации (установка камер и введение электронных штрафов) и т. д. Практически в каждой из перечисленных сфер жизнедеятельности, используются персональные данные конкретного человека. К большому сожалению, эти данные не имеют должной, в том числе и уголовно-правовой защиты, от возможного их использования против интересов конкретной личности, так и в преступных целях, представляющих угрозу общественной безопасности.

Глава 28 Уголовного кодекса Российской Федерации устанавливает ответственность за деяния, связанные с осуществлением преступных посягательств в информационной сфере. К таким общественноопасным посягательствам (ст.ст. 272, 274.2 УК РФ) относят: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств, хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

¹ © Еремина А. А. 2025.

В результате ужесточения законодательства в области посягательств, связанных с компьютерной информацией, появился новый состав преступления, связанный с неправомерным использованием компьютерной информацией, *содержащей персональные данные*, регламентированный ст. 272.1 УК РФ (ФЗ № 421 от 30.11.2024). По мнению российского ученого Чернышева А. В., «Проблема неправомерного доступа к компьютерной информации требует комплексного подхода. Необходимо усилить контроль за соблюдением законов в области информационной безопасности, а также развивать образовательные программы, направленные на повышение осведомленности граждан о рисках, связанных с использованием цифровых технологий» [1].

Понятие «компьютерная информация» дано в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также в примечании к ст. 272 УК РФ, где указано, что она представляет собой сообщения, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Рассматривая состав данного преступления, а именно посягательства, связанные с *незаконным использованием, хранением и передачей компьютерной информации, содержащей персональные данные*, анализируя его элементы и признаки, необходимо акцентировать особое внимание на тех признаках, которые позволяют говорить о своевременности и актуальности дополнительной правовой регламентации таких преступных посягательств.

К родовому объекту данного состава преступления относят общественные отношения, регулирующие общественную безопасность. Видовым объектом являются общественные отношения, складывающиеся по поводу правомерного пользования компьютерной информацией. Основным непосредственным объектом являются общественные отношения, которые обеспечивают законный доступ, создание, хранение, модификацию и использование компьютерной информации, *содержащей персональные данные*. Дополнительным непосредственным объектом будут выступать конституционные права на гарантии сохранности личной, персональной информации. Факультативным объектом могут являться отношения, осуществляющие охрану собственности и интересов государственной службы и службы в коммерческих структурах.

Исходя из положений ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ, под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, то есть субъекту персональных данных, поэтому к предметам, на которые направлено данное общественноопасное посягательство, относится:

1) персональные данные [2], в том числе несовершеннолетних лиц (сведения, содержащиеся в свидетельстве о рождении; персональная информация, содержащаяся в личном деле обучающегося и в классном журнале и электронном дневнике);

2) биометрические данные пользователя (физиологические и биологические особенности человека, на основании которых можно установить его личность);

3) специальные категории персональных данных (данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений).

Анализируя в общем деяния, связанные с неправомерным использованием компьютерной информации, необходимо отграничить это определение, от понятия компьютерной техники. Где в качестве последнего определения признаются все устройства, связанные с обработкой компьютерной информации, а именно: персональные компьютеры, смартфоны, персональные компьютерные планшеты, кассовые аппараты, банкоматы, а также иные устройства. Таким образом, если будет дополнительно причинен материальный вред, в виде технической неисправности устройству, связанному с обработкой, передачей компьютерной информации, то необходима дополнительная квалификация, с учетом имущественного ущерба.

Существенным фактором для правильной уголовно-правовой оценки в этих случаях, выступает то, что диспозиция рассматриваемой статьи является бланкетной и необходимо обращаться к иным нормативным правовым актам. Кроме вышеперечисленных нормативных актов, учитывать необходимо положения ГК РФ, нормативную базу, связанную с трансграничной торговлей и т. д.

Рассматривая структуру объективной стороны по ч. 1. ст. 272.1 УК РФ состав является формальным, то есть преступление будет считаться оконченным, при выполнении одного или нескольких, или же всей совокупности указанных в диспозиции действий. Для квалифицированных частей, предполагается возможность формально-материальной конструкции.

В основном составе рассматриваемой ст. 272.1 УК РФ объективная сторона выражена новой совокупностью действий, где кроме неправомерного доступа и использования компьютерной информации, содержащей сведения личного характера, могут присутствовать также общественно-опасные деяния, связанные с вмешательством в функционирование средств, хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Вышеуказанные действия представляют собой целенаправленное программное воздействие на персональные компьютеры, серверы, информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации [3].

Квалифицированными рассматриваемые действия будут, если потерпевшим окажется несовершеннолетнее лицо. Также как квалифицированные такие действия будут оцениваться в зависимости от специфики определенной категории персональных данных, то есть данных, отнесенных к специальным и (или) биометрическим персональным данным. Возраст потерпевшего и специфика персональных данных, естественно, повышают степень общественной опасности содеянного и требует повышенной уголовной ответственности.

Особо квалифицированными такого рода действия, признаются при установлении корыстного мотива, причинения крупного ущерба или наступления тяжких последствий, использования служебных полномочий. Также данные общественноопасные деяния совершаются лицами по предварительному сговору или

организованной группой. Что, в свою очередь, влечет еще более суровый подход в установлении вида и размера наказания.

Отдельно следует рассмотреть такие особо квалифицированные части рассматриваемого состава преступления, как деяния, сопряженные, с трансграничной передачей личных данных и создание ресурса для незаконной передачи, хранения компьютерной информации, которая содержит персональные данные, добытые незаконным путем, в том числе и биометрические персональные данные.

В ч. 4 ст. 272.1 УК РФ предусмотрена ответственность за преступные деяния, связанные с трансграничной передачей, компьютерной информации, в том числе, содержащий персональные данные, отнесенные к специальным, биометрическим персональным данным. Для чего и в каких целях могут быть использованы такие данные за пределами Российской Федерации, можно только предполагать. Например, эти данные, могут быть использованы для шантажа, определенной категории граждан РФ, ввиду занимаемой ими должности, служебного, общественного положения. А также для проведения, в том числе и в сопредельных странах, разнообразных биологических опытов. Естественно, такие утечки представляют реальную угрозу общественной безопасности в РФ и требуют соответствующей уголовно-правовой оценки.

В ч. 6 ст. 272.1 УК РФ, речь идет о создании ресурса для незаконной передачи, хранения компьютерной информации, которая содержит персональные данные, которые получены незаконным путем. Создание и поддержка дальнейшего функционирования такого ресурса предполагают привлечение значительных материальных и технических составляющих, позволяющих оперировать большими объемами такого рода информации, полученной преступным путем, для дальнейшего ее использования в преступных целях. Все это позволяет оценивать такие действия, как особо квалифицированные, ставящие под угрозу общественную безопасность в стране.

О направленности умысла на совершения преступлений именно против общественной безопасности в более широком смысле, то есть не только в рамках видового объекта, позволяет говорить значимость рассматриваемого предмета преступного посягательства, степень общественной опасности способов и методов, применяемых для достижения преступного результата [4].

1. *Персональные данные* – такого рода преступления, связанные с компьютерной информацией, представлены особым предметом, в виду специфики информации, где речь идет об индивидуальных данных конкретного человека. Но из-за способа завладения этой информацией, скорости ее обработки и передачи, получить и затем использовать в преступных целях можно информацию, содержащую персональные данные, в том числе и биометрические данные, неопределенно широкого круга лиц. Печально, когда эти данные используются в мошеннических схемах, намного серьезней ситуация, если такого рода данные используются для фальсификации голосования электронным способом.

2. *Действия, направленные на передачу персональных данных*, – это совокупность действий, связанных в том числе, с продажей, размещением их на серверах, предназначенных для удаленного обмена файлами, предоставлением персо-

нальных данных по запросам, предоставлением возможности обращения к источнику хранения информации с персональными данными конкретным лицам или неопределенному кругу лиц, а также иных преступных действий.

3. *Действия, направленные на сбор персональных данных*, — это деятельность по систематизации, накоплению, уточнению и извлечению персональных данных.

4. *Действия, связанные с хранением персональных данных*, — это совершение любых действий, связанных с нахождением данных сведений в фактическом пользовании и владении лица.

Важнейшими характеристиками этих всех действий, направленных на достижения преступного результата, является скорость, как передачи, так и сбора соответствующей информации, возможности хранения и оперативной обработки огромнейшего объема такого рода данных. Все вышеперечисленное самым непосредственным образом влияет на определение как характера, так и степени общественной опасности таких преступлений. Все вышеперечисленное позволяет утверждать о целесообразности и своевременности реагирования со стороны законодателя в отношении такого рода преступных посягательств.

При осуществлении сравнения статьей 272.1 и 272 УК РФ необходимо выделить, что объективная сторона последнего состава выражена в неправомерном доступе, а именно незаконном доступе к личной информации, что является общественноопасным деянием. Общественноопасным последствием являются уничтожение, блокирование, копирование и модификация информации, являющейся собственностью гражданина и наличие причинной связи как обязательный признак, связывающий преступное деяние и последствие. В данном случае неправомерный доступ считается оконченным с момента, когда субъект преступления может распоряжаться информацией лица, в отношении которого направлено преступление. В ст. 272.1 УК РФ объективная сторона, кроме вышеуказанного в рамках неправомерного доступа, включает дополнительные преступные деяния, касающиеся систем хранения, обработки информации персональных компьютеров и компьютерных систем.

Рассматривая ч. 2 ст. 272 УК РФ данная норма представляет собой наступление уголовной ответственности за причинение, в результате преступных действий, крупного ущерба, который в соответствии с примечанием данной статьи, превышающий более 1 миллиона рублей. Корыстная заинтересованность заключается в стремлении виновного получить для себя или других лиц выгоду имущественного характера, либо избавиться от материальных затрат. При этом ответственность за совершение подобных деяний предусмотрена под пунктами «а» и «б» ч. 3 ст. 272.1 УК РФ, что является важным фактором при квалификации преступных действий и является проблемой при разграничении данных составов [5].

В ч. 3 ст. 272 УК РФ предусмотрена ответственность за совершение данного общественноопасного деяния, совершенного группой лиц по предварительному сговору, организованной группой либо лицом с использованием своего служебного положения. Рассматривая совершение данного преступления группой лиц по предварительному сговору, то в данном случае обязательным признаком является договоренность между лицами о совершении неправомерного доступа.

Совершение общественноопасного деяния организованной группой как квалифицирующий признак проявляется в случае установления устойчивости данной группы, направленной на совершение подобных преступлений. Рассматривая признак, связанный с использованием своего служебного положения, то необходимо отметить, что у лица, совершающего данное преступление, должны быть соответствующие полномочия, которые он осознанно нарушает с целью совершения данного общественноопасного деяния.

В части 4 статьи 272 УК РФ предусмотрена ответственность за совершение вышеуказанных деяний, если они повлекли наступление тяжких последствий или угрозу наступления тяжких последствий. Тяжкие последствия являются оценочным признаком и должны устанавливаться конкретно законодателем. Тяжкими последствиями по уголовному законодательству Российской Федерации является причинение смерти, смерти по неосторожности, тяжкого и среднего вреда здоровью т. д.

Проведенный анализ позволяет утверждать, что инициатива законодателя, в части уголовно-правовой регламентации преступлений, связанных с неправомерным использованием компьютерной информацией, *которая содержит личные данные граждан*, (ст. 272.1 УК РФ), является, безусловно, правильной и своевременной. Состав преступления, регламентированный статьей 272.1 УК РФ, направлен на привлечение к уголовной ответственности лиц, совершивших неправомерное использование компьютерной информации, представляющей личные данные, в достаточно широком и специфическом диапазоне. Ко всему прочему, наряду со специфическим предметом преступления, повышенную общественную опасность представляют описанные в данной статье действия.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 06.10.2022.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 12.10.2023) // СЗ РФ от 17 июня 1996 г., № 25, ст. 2954.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, // Российская газета – Федеральный выпуск: № 4131, 29 июля, 2006.
4. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"» // Российская газета – Федеральный выпуск: № 8942, 28 декабря, 2022.
5. Кадников Н. Г. Уголовное право России: Учебник. Том 1. / Общая часть. Москва. Юриспруденция. 2018. – 944 с.

6. Дмитренко А. П. Уголовное право: Курс лекций / Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя. Москва. 2022. – 80 с. (дата обращения: 17.04.2025).
7. Бавсун М. В., Векленко С. В. Квалификация преступлений по признакам субъективной стороны: Учебник для вузов. / М: Юрайт. 2024. – 144 с.
8. Боровиков В. Б., Смердов А. А. Уголовное право: Учебник для вузов. Общая часть. / М.: Юрайт. 2023. – 269 с.
9. Интернет-сайт «Право.Ру». // Научная электронная библиотека. URL: <https://pravo.ru/news/240437/amp/>. (дата обращения: 02.05.2025).
10. Обзор судебной практики Верховного Суда Российской Федерации № 2 (2021). (утв. Президиумом Верховного Суда РФ 30.06.2021) // сайт Верховного суда Российской Федерации. URL:<https://www.consultant.ru>. (дата обращения: 02.05.2025).
11. Харламова А. А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации / Караваев Н. А. // Молодой ученый. 2023. № 23. С. 338–340.
12. Мамочка Е. А. Уголовно-правовое противодействие неправомерному использованию инсайдерской информации / Е. А. Мамочка // Пробелы в российском законодательстве. 2014. № 4. С. 121–124.
13. Караваев Н. А. Неправомерный доступ к компьютерной информации: проблемы квалификации / Н. А. Караваев. // Молодой ученый. — 2023. № 23 (470). С. 338–340.
14. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Ермакова А. С.¹,

курсант института подготовки сотрудников

для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Михайленко Н. В.,

доцент кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ РАЗВИТИЯ КУЛЬТУРЫ СОЦИАЛЬНОГО ВЗАИМОДЕЙСТВИЯ С НАСЕЛЕНИЕМ У СОТРУДНИКОВ ПОЛИЦИИ

Современное общество характеризуется высоким уровнем цифровизации, что оказывает непосредственное влияние на все сферы жизни, в том числе на деятельность правоохранительных органов. Для полиции важно не только эффективно реализовывать функции охраны правопорядка, но и выстраивать доверительные и устойчивые отношения с населением. В этих условиях особое значение приобретает развитие культуры социального взаимодействия у сотрудников органов внутренних дел, основанной на открытости, диалоге и уважении к правам граждан. Этому в значительной мере способствует использование современных информационно-коммуникационных технологий (ИКТ), позволяющих налаживать эффективную коммуникацию между полицией и обществом.

Культура социального взаимодействия сотрудников полиции – это совокупность норм, ценностей и моделей поведения, определяющих характер их общения с гражданами, уровень уважения к личности, соблюдение прав и свобод, а также способность к диалогу и разрешению конфликтов. Она является важнейшим элементом профессиональной культуры и напрямую влияет на уровень доверия к органам правопорядка.

Развитие данной культуры предполагает не только совершенствование коммуникативных навыков, но и внедрение практик, ориентированных на учет общественного мнения, прозрачность деятельности, использование обратной связи и активное участие граждан в профилактике правонарушений. Именно здесь ИКТ становятся важным инструментом.

Под ИКТ понимается комплекс технологий, обеспечивающих сбор, передачу, хранение и обработку информации. Для полиции это, прежде всего, цифровые платформы, официальные сайты, социальные сети, системы видеонаблюдения, «горячие линии», мобильные приложения, а также электронные формы опросов и анкетирования.

¹ © Ермакова А. С., 2025.

Наиболее активно ИКТ используются в следующих направлениях:

- распространение информации о деятельности полиции (новости, профилактика, отчеты);
- прием обращений граждан в электронной форме;
- ведение официальных аккаунтов в социальных сетях;
- проведение опросов общественного мнения;
- организация общественного контроля;
- формирование «цифрового имиджа» органов МВД России.

Использование ИКТ способствует расширению каналов коммуникации с обществом и делает деятельность полиции более открытой и прозрачной. Сотрудники органов внутренних дел получают возможность быстро реагировать на обращения граждан, вести разъяснительную работу, опровергать недостоверную информацию и демонстрировать готовность к сотрудничеству.

Кроме того, через цифровые технологии возможно выявление «болевых точек» во взаимодействии с обществом: анализируя данные обращений, комментариев и анкет, руководство может принимать обоснованные управленческие решения.

ИКТ также позволяют осуществлять просветительскую и правовую работу, формируя у населения правосознание, уважение к закону и правопорядку. Немаловажным является и влияние на формирование внутренней мотивации сотрудников — они начинают осознавать важность социальной составляющей своей профессии.

Несмотря на очевидные преимущества, процесс внедрения ИКТ сопровождается рядом проблем:

- недостаточный уровень цифровой грамотности у части сотрудников;
- формализм в ведении социальных сетей и онлайн-коммуникации;
- риск утечки служебной информации;
- недоверие со стороны части граждан к электронным каналам связи;
- отсутствие единых стандартов ведения диалога в цифровой среде.

Также возникает опасность подмены живого общения формальной онлайн-отчетностью, что может привести к отчуждению граждан, особенно в социально уязвимых группах.

Для повышения эффективности применения ИКТ в целях формирования культуры социального взаимодействия с населением целесообразно:

- систематически обучать сотрудников полиции цифровой коммуникации и основам медиаграмотности;
- развивать платформы обратной связи и электронного консультирования;
- внедрять элементы искусственного интеллекта для анализа общественного мнения;
- формировать положительный имидж полиции через цифровые медиаресурсы;
- поощрять инициативность сотрудников в установлении конструктивного диалога с гражданами.

Важную роль также играет вовлечение молодежи и общественных организаций в цифровые формы взаимодействия с полицией.

Для глубокого понимания возможностей применения ИКТ в развитии культуры взаимодействия между полицией и гражданами полезно обратиться к опыту зарубежных стран. В ряде государств сформировались эффективные практики использования цифровых технологий как инструмента открытости и доверия.

В США, например, функционирует широкая сеть цифровых платформ, на которых местные полицейские управления публикуют отчеты о своей деятельности, данные о преступности, разъяснительные материалы и инструкции для граждан. Большое внимание уделяется социальным сетям, через которые органы правопорядка не только информируют население, но и собирают обратную связь, проводят интерактивные консультации и оперативно реагируют на запросы.

В Великобритании активно применяется концепция «цифрового сообщества» (Digital Policing), согласно которой каждому району соответствует онлайн-представительство, где граждане могут обсудить насущные проблемы, направить жалобы, принять участие в виртуальных слушаниях или мероприятиях. Таким образом, достигается эффект сопричастности общества к обеспечению правопорядка.

Ярким примером применения ИКТ в интересах доверительного взаимодействия является проект «Smart Policing» в Сингапуре, где используются системы видеоаналитики, мобильные приложения для жалоб, а также платформа искусственного интеллекта, анализирующая общественные настроения в интернете. Эти технологии не заменяют человеческий контакт, а усиливают его, подчеркивая внимание государства к запросам общества.

Российский опыт внедрения аналогичных технологий пока не столь масштабен, однако имеет потенциал к развитию при условии целенаправленного подхода и анализа лучших мировых практик.

Значительная часть формирования культуры взаимодействия сотрудников полиции с населением осуществляется в ходе профессиональной подготовки. В вузах системы МВД России обучение должно быть ориентировано не только на правовые и тактические аспекты служебной деятельности, но и на развитие цифровой и коммуникативной компетентности будущих сотрудников.

В рамках учебных дисциплин и специальных курсов необходимо:

- формировать представления о сущности информационно-коммуникационных технологий;
- обучать навыкам ведения официальной цифровой коммуникации;
- моделировать ситуации диалога с гражданами через цифровые каналы;
- развивать этическое сознание и медиаграмотность.

Особое значение имеет вовлечение курсантов в проектную и исследовательскую деятельность, связанную с цифровыми средствами обратной связи, системами «электронной полиции», созданием обучающих роликов и инфографики для социальных сетей. Такая активность не только укрепляет профессиональные навыки, но и стимулирует осознанное отношение к миссии правоохранительных органов в условиях цифрового общества.

Цифровое общение существенно отличается от традиционного. Оно опосредовано технологическим интерфейсом и лишено многих невербальных компонентов, что может искажать восприятие, снижать эмпатию или вызывать агрессию. Поэтому культура цифрового общения требует от сотрудников полиции дополнительных компетенций, в том числе:

- умения понимать контекст и эмоциональное состояние собеседника на основе текста;
- соблюдения нейтрального и уважительного тона;
- способности к саморефлексии и управлению репутацией в цифровой среде.

Кроме того, важно учитывать психологическое давление, которое могут испытывать сотрудники при массовых критических комментариях или информационных атаках. Это требует наличия внутренних регламентов психологической поддержки, а также умения «выдерживать удар» и сохранять профессионализм в любых условиях общения.

Одним из приоритетных направлений является формирование устойчивого цифрового партнерства между полицией и институтами гражданского общества. Для этого необходимо не просто предоставлять информацию, но и активно вовлекать население в процесс принятия решений и профилактики правонарушений.

На практике это может выражаться в:

- регулярных онлайн-опросах по вопросам общественной безопасности;
- виртуальных общественных советах;
- участии граждан в обсуждении локальных проблем через городские порталы;
- взаимодействии с блогерами, общественными активистами и родительскими сообществами.

Таким образом, современные ИКТ не только обеспечивают технические условия для коммуникации, но и становятся инструментом формирования новой модели взаимодействия.

Информационно-коммуникационные технологии становятся неотъемлемой частью современной правоохранительной практики и важным ресурсом для формирования культуры социального взаимодействия у сотрудников полиции. Их грамотное применение позволяет укреплять доверие общества, повышать эффективность профилактической работы и формировать имидж полиции как открытой, ориентированной на гражданскую поддержку структуры. Вместе с тем успех этого процесса зависит от профессиональной подготовки сотрудников, институциональной поддержки и системного подхода к цифровой трансформации правоохранительной деятельности.

Список литературы

1. Баринов П. А. Информационно-коммуникационные технологии в правоохранительной деятельности: учебное пособие / П. А. Баринов. – М.: ЮНИТИ-ДАНА, 2021. – 240 с.

2. Васильев И. В. Культура общения сотрудников полиции с населением: монография / И. В. Васильев. – СПб.: Питер, 2020. – 184 с.
3. Зубарев С. А. Цифровые технологии и право: вызовы и решения / С. А. Зубарев // Журнал российского права. – 2023. – № 11. – С. 54–61.
4. Официальный сайт МВД России [Электронный ресурс]. – Режим доступа: <https://мвд.рф>.
5. Хуторской А. В. Коммуникативная культура и цифровое общество / А. В. Хуторской // Социальные и гуманитарные науки. – 2022. – № 4. – С. 88–95.
6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
7. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
8. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
9. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
10. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.
11. Расследование преступлений, совершенных с использованием криптовалюты: учебное пособие / Д. А. Иванов, М. М. Макаренко, В. В. Пушкарёв, Е. А. Рускевич. – Москва : Ай Пи Ар Медиа, 2021. – 80 с.
12. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарёв, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Ермакова П. А.¹,

курсант института подготовки сотрудников

для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Константинов А. В.,

заместитель начальника кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ПРАВОВАЯ ХАРАКТЕРИСТИКА «ВЕБКАМ-ИНДУСТРИИ» КАК ПРЕСТУПНОЕ ЯВЛЕНИЕ В ИНТЕРНЕТЕ

С уверенностью можно утверждать о том, что вебкам-индустрия – это принципиально новая форма интерпретации, которая предусматривает предоставление интим-услуг в рамках цифрового пространства [1]. Глобальное распространение таких услуг среди населения, развитие многочисленных информационных технологий позволяет активно использовать вебкам, как коммерчески массовое мероприятие. После того, как стартовала так называемая третья волна развития вебкама (сначала на начальном этапе был заимствован западный опыт; на втором этапе им заинтересовалась отечественная молодежь, как способ быстрого заработка), после появления пандемии коронавируса интерес к указанному явлению только увеличился [2].

Если детально рассматривать сущность вебкам, то оно представляет собой оказание онлайн услуг коммерческого, сексуального характера в режиме реального времени. Веб-модель ведет общение со зрителем в видеочате, чтобы удовлетворять, как сексуальные, так и прочие потребности самого зрителя. Такие сеансы организуются на сайтах, тематических платформах. Однако практически квалифицировать соответствующие деяния весьма проблематично, так как применяются всевозможные средства анонимности в Интернете, специальные средства трансляции. Кроме прочего, субъекты деятельности выходят на международный уровень [3]. Известно о том, что веб-модели могут работать исключительно на сайтах двух типов:

1. Премиум – где доход получают от частных комнат.

2. Freemium – в данном случае доходы – это добровольные донаты, посредством бесплатных чатов. Тут контент с сексуальным подтекстом не запрещен. В качестве примера можно представить такие площадки, как OnlyFans, «видео-девочка», LiveJasmine, Chaturbate, Bongacams и Streamate и так далее. Также нужно отметить, что некоторые из заявленных выше ресурсов уже были внесены в Рос-

¹ © Ермакова П. А., 2025.

сии в реестр запрещенной информации на основаниях, которые прописаны в Законе «Об информации и информационных технологиях», в статье 15.1. Для этого выносились решения судов. Впрочем, российский пользователь продолжает там регистрацию, так как применяются прокси-серверы, анонимайзеры и прочие инструменты анонимности.

Известно о том, что модель может работать на индивидуальной основе или посредством вебкам агентства, которое обеспечивает не только техническую базу, но и материальную стабильную поддержку. Так, если модель заключает со студией контракт, то это значительно упрощает ее работу, так как управленческие функции, поиск и обустройство «места работы» для трансляций, создание учетной записи, активация аккаунта – всем этим занимаются специально обученные люди [4]. Среди сотрудников студий очень часто можно выделить собственников и администраторов, видеографов, менеджеров по поиску моделей, криэйторов, которые разрабатывают шоу-программу, образы самих моделей. Добавим, что вебкам-агентства работу выстраивают с применением техники, различного оборудования, которое может применяться в целях совершения высококачественных трансляций. Это высокоскоростной доступ в интернет, профессиональное освещение, камеры, регистрация и создание профилей на сайтах, поиск клиентов и многое другое [5].

Существует два компонента, на которых базируется явление «вебкам» – специализированные сайты, а также платежные электронные системы (в том числе банки), которые выступают в качестве посредников для оказания финансовых услуг. Кроме прочего, нами был проанализирован дополнительный компонент – поисковые системы по изображению (сопоставление лица человека). На данный момент информационные технологии дают возможность организовать видеосвязь между зрителем и моделью на конфиденциальных условиях. Считается, что в анализируемой индустрии – это основной компонент. Работают сайты с открытым доступом, посредством которых оплачиваются услуги модели, передаются средства в банки, где в дальнейшем могут быть выведены в наличность.

Как утверждает Е. В. Берсенева [6], именно отсюда начинается распространение видеоматериалов порнографического характера в режиме онлайн через Интернет. ведь участие в зрелищных мероприятиях порнографии предусматривает онлайн видеоконтакт. Отмечаем, что в отечественном уголовном праве была колоссальная проблема, когда стояла задача – квалифицировать анализируемое деяние. Ведь анонимность трансляции, которая ведется через специальные сайты, не дает привязки к личности.

С уверенностью утверждаем о том, что вебкам-индустрия – это совершенно новая форма по интерпретации предоставления интимных услуг посредством цифровых инструментов. Глобальное развитие, распространение цифровых технологий среди населения позволяет на данный момент активно внедрять вебкам в коммерческое, массовое сознание.

Итак, если рассматривать понятийную базу самого явления «вебкам», то свое начало она берет с аналогичного термина. Вебкам моделинг является конкретной формой предоставления услуг, взамен которых можно получить прибыль. Для этого осуществляется трансляция эротического или порнографического контента

в режиме онлайн с компонентами общения. Модель оказывает услугу, но пользователя видеть не может. Так как анализируемое явление характеризуется своей колоссальной вариативностью, то могут быть некоторые отклонения. Впрочем, даже в приближенности можно проследить его сущность. Это усредненный вариант между проституцией и созданием порно-материалов [7]. Вокруг вебкам складывается некоторый понятийный аппарат – объекты, предметы, а также субъекты. Вебкам модель является физическим лицом, которое занимается предоставлением порнографических или эротических услуг, что не основано на личных симпатиях, на влечении. Главная цель заключается в получении выгоды. Клиент или мембер, пользователь – лицо, которое использует услуги вебкам модели. Есть также вебкам студия, как компания, которая привлекает моделей, организует работы и материальную базу; это посредник, который получает свою часть доходов.

В составе материальной базы можно выделить такие компоненты, как рабочее помещение, мебель в нем, компьютеры, средства видеотрансляции, освещение и так далее.

Вебкам комната представляет собой виртуальную ячейку, пространство на сайте для трансляции видеоконтента от модели, с персонального аккаунта. Токен – есть внутренняя валюта, которую покупают клиенты, мемберы за реальные деньги, чтобы потом оплатить услуги моделей [8].

Характерная черта выделения, а также перспективного документирования его выражается в получении сведений разными способами, которые предусматриваются проведением розыскных, оперативных мероприятий. Так, может быть задействован прямой аналитический, информационный поиск оперативной и релевантной информации в Интернете. Масштабно, однако не конкретизировано можно получить данные от лиц, которые ведут негласное сотрудничество с ОВД. К оперативно-розыскным мероприятиям очень часто привлекаются администраторы, модели, прочие участники работы вебкам студий. Все это дает возможность сформировать картину о противоправности деятельности от субъектов, получить доказательственную базу не только для возбуждения уголовного дела, но и для предоставления доказательств виновной стороны в суде. Как видим, вовсе не требуется комплексная процедура, связанная с подготовкой, а также внедрением агентуры, так как главная задача – найти и завербовать [9]. Очень редкий случай – получение информации, которая исходит от родственников или соседей, самих моделей, которые стали жертвами раскрытия своей деятельности в указанной индустрии [10].

В представленной выше ситуации оперативная работа будет сведена к стандартизированным процедурам, к проведению оперативно-розыскных мероприятий. То есть, осматриваются места происхождения, вебкам студии; оформляются выписки с банковских счетов моделей, администраторов студий. Оперативно-розыскные мероприятия преследуют следующие цели [11]:

1. Установить круг лиц, которые принимают непосредственное участие в работе вебкам; приоритетное внимание получают несовершеннолетние лица, способы их привлечения к указанной деятельности, а также установление фактов сексуальной эксплуатации.

2. Способы, посредством которых рассчитываются клиенты со студией – иностранная валюта, криптовалюта, прочие аналогичные способы, посредством которых можно конвертировать цифровые деньги в реальные средства. Далее определяются пути, сайты, расчетные счета на платежных системах, рынки криптовалюты, что приравнены к услугам соответствующего характера; обменники.

3. Проверить существование каналов связи, при согласованном транслировании детской порнографии через некоторые сайты. В качестве подобных каналов могут выступать форумы на платформах -.onion либо telegram-каналы, прочие средства коммуникации с общественностью.

4. Установить айпи адреса, или непосредственно лиц, которые пользуются услугами вебкам студий; лиц, которые распространяют детское порно.

5. Собрать материальные носители, получить доступ к хранилищам, на которых могут быть сконцентрированы порнографические материалы, привязать записанный материал к лицам, которые создавали контент. Привязать лиц к ПК вебкам студий.

Так как можно установить факты противоправной деятельности, то правильно будет технически зафиксировать все обстоятельства, посредством которых в дальнейшем удастся правильно раскрыть преступление, определить виновность лица в преступлении.

Список литературы

1. Берсенева Е. В. Отношение уголовного закона Российской Федерации к явлению «вебкам» // Вопросы российской юстиции. – 2021. – № 15. – С. 487.

2. В Волгограде полицейскими пресечена деятельность организованной группы, занимавшейся изготовлением порнографических материалов [Электронный ресурс]. URL: <https://xn--b1aew.xn--p1ai/news/item/17170783/> (дата обращения: 15.01.2025).

3. Ваганова М. А., Копейка А. Н. Уголовно-правовое регулирование виртуальной проституции // Эволюция российского права. Екатеринбург, 2022. – С. 786.

4. Ваганова М. А., Копейка А. Н. Уголовно-правовое регулирование виртуальной проституции // Эволюция российского права. Екатеринбург, 2022. – С. 788.

5. Дворянкин О. А. Новейшие интернет-технологии, комплексно обрабатывающие современных людей // Национальная ассоциация ученых. – 2020. – № 58-2 (58). – С. 4.

6. Евсеева Я. В. Интимность в эпоху интернета // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 11, Социология: Реферативный журнал. – 2020. – № 4. – С. 38.

7. Енгальчев В. Ф., Зайцева О. В. Выявление объектов детской порнографии в виртуальном пространстве посредством дешифровки наименований и тегов // Вестник Томского государственного университета. – 2021. № 471. – С. 236.

8. Жданов Ю. Н., Овчинский В. С. Кибермафия как объект оперативно-розыскного воздействия / Ю. Н. Жданов // Оперативно-розыскная деятельность в цифровом мире. – 2021. – С. 38.

9. Полиция задержала восемь человек, которых обвинили в организации вебкам-студии в Красноярске. Им вменили создание преступного сообщества [Электронный ресурс]. URL: <https://tauga.info/165106> (дата обращения: 15.01.2024).

10. Смирных С. Е. Международное сотрудничество в борьбе с коррупцией как гарантия предупреждения торговли детьми / С. Е. Смирных // Российская юстиция. – 2020. – № 12. – С. 16.

11. Шарапов Р. Д. Квалификация преступлений, связанных с незаконным оборотом порнографических материалов и предметов / Р. Д. Шарапов // Законность. – 2021. – № 8(1042). – С. 43.

12. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

13. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

14. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

15. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

16. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

17. Пушкарев В. В. Реализация уголовного преследования в условиях цифровой экономики: легализация (отмывание) доходов, полученных преступным путем, с помощью стэйблкоинов / В. В. Пушкарев // Самоуправление. – 2019. – Т. 2. – № 1 (114). – С. 287–289. – EDN ZAQTVB.

Зайцева Е. А.¹,

курсант института

подготовки сотрудников для органов

предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Поликарпова Е. В.,

старший преподаватель

кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя

ПОРЯДОК ПОЛУЧЕНИЯ ГОЛОСОВОЙ ИНФОРМАЦИИ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ МОБИЛЬНОЙ СВЯЗИ И ИТ-ТЕХНОЛОГИЙ

В настоящее время почти каждый человек использует мобильную связь и информационные технологии. Мобильные устройства и сеть Интернет стали неотъемлемой частью жизни во всех сферах, которые позволяют пользователям использовать огромный объем данных. Но с стремительным развитием информационных технологий возникают и новые вызовы в аспекте безопасности. Одной из главных проблем является применение мобильной связи и ИТ-технологий для получения голосовой информации.

В современных условиях развития информационных технологий особое значение приобретает исследование методов и способов получения голосовой информации с использованием мобильных средств связи и инновационных информационных технологий. Данный процесс представляет собой комплексную систему, включающую в себя множество технологических, правовых и организационных аспектов, требующих детального рассмотрения и анализа.

Технологический процесс получения голосовой информации начинается с момента формирования звукового сигнала источником речи. При этом происходит первичное преобразование акустического сигнала в электрический посредством микрофона, установленного в мобильном устройстве. Важно отметить, что качество первичного преобразования во многом определяет конечное качество передаваемой голосовой информации. Современные микрофоны оснащаются встроенными цифровыми фильтрами и системами шумоподавления, что позволяет существенно повысить качество исходного сигнала.

После аналого-цифрового преобразования полученный цифровой сигнал подвергается процессу компрессии и кодирования. На данном этапе применяются различные алгоритмы сжатия данных, среди которых наиболее распространены G.711, G.729 и AMR. Выбор конкретного алгоритма зависит от требуемого каче-

¹ © Зайцева Е. А., 2025.

ства передачи и пропускной способности канала связи. При этом важно учитывать, что чрезмерное сжатие может привести к потере качества голосовой информации, а недостаточное сжатие – к неэффективному использованию канала передачи данных.

Передача закодированного голосового сигнала осуществляется через сеть мобильной связи, которая представляет собой сложную многоуровневую структуру. В современных условиях активно развиваются технологии 4G и 5G, обеспечивающие значительно более высокие скорости передачи данных по сравнению с предыдущими поколениями мобильной связи. При этом важным аспектом является обеспечение качества обслуживания (QoS), которое достигается за счет приоритетной обработки голосовых пакетов данных и минимизации задержек при передаче.

На стороне получателя происходит обратный процесс декодирования и восстановления исходного голосового сигнала. Современные мобильные устройства оснащены специализированными процессорами обработки сигналов, которые обеспечивают высокую скорость декодирования и минимальное энергопотребление. После восстановления цифрового сигнала происходит его преобразование в аналоговый формат с последующей передачей на динамики устройства.

Особое внимание следует уделить вопросам безопасности при получении голосовой информации. В современных условиях активно применяются различные методы шифрования голосовых данных, среди которых наиболее распространены протоколы SRTP и ZRTP [1, с. 384]. Данные протоколы обеспечивают защиту от несанкционированного доступа к передаваемой информации и предотвращают возможность перехвата голосовых данных третьими лицами.

Важным аспектом является также аутентификация участников голосового общения. Современные мобильные устройства поддерживают различные методы биометрической аутентификации, включая распознавание голоса, что существенно повышает уровень защищенности голосовых коммуникаций. При этом процесс аутентификации происходит автоматически и не создает дополнительных неудобств для пользователя.

В контексте развития информационных технологий особое значение приобретает интеграция голосовых коммуникаций с другими сервисами и приложениями. Современные мобильные платформы поддерживают возможность автоматического распознавания речи и преобразования ее в текстовый формат, что открывает новые возможности для обработки и анализа полученной информации.

При получении голосовой информации посредством мобильной связи необходимо учитывать ряд технических ограничений. Одним из ключевых факторов является качество канала связи, которое может существенно варьироваться в зависимости от местоположения пользователя и загруженности сети. Для минимизации негативного влияния данных факторов применяются различные методы адаптивной модуляции и кодирования, позволяющие автоматически подстраиваться под текущие условия канала связи.

Важным аспектом является также энергопотребление при осуществлении голосовых коммуникаций. Современные мобильные устройства оснащаются специальными режимами энергосбережения, которые позволяют оптимизировать расход заряда батареи при передаче голосовых данных. При этом происходит динамическое управление мощностью передатчика и частотой опроса сети в зависимости от текущих условий связи.

В условиях развития облачных технологий особое значение приобретает возможность хранения и обработки голосовой информации на удаленных серверах. Современные облачные платформы обеспечивают высокую надежность хранения данных и возможность их обработки с использованием мощных вычислительных ресурсов. При этом важным аспектом является обеспечение конфиденциальности хранимой информации и защита от несанкционированного доступа.

Особого внимания заслуживает вопрос стандартизации процессов получения голосовой информации. Международные организации по стандартизации разрабатывают и обновляют стандарты, регламентирующие различные аспекты голосовых коммуникаций, включая качество передачи, методы шифрования и протоколы взаимодействия. Соблюдение данных стандартов обеспечивает совместимость различных систем и устройств, что является необходимым условием для развития современных телекоммуникаций.

В контексте развития искусственного интеллекта особое значение приобретает возможность автоматической обработки и анализа полученной голосовой информации. Современные системы машинного обучения позволяют осуществлять распознавание речи, определение эмоционального состояния, говорящего и даже идентификацию личности по голосу. Данные технологии находят применение в различных сферах, включая обслуживание клиентов, медицинскую диагностику и обеспечение безопасности.

При организации процесса получения голосовой информации необходимо учитывать законодательные требования, регулирующие обработку персональных данных и защиту конфиденциальной информации. В большинстве стран действуют специальные нормативные акты, регламентирующие порядок хранения и передачи голосовой информации, а также ответственность за нарушение установленных требований.

В современных условиях активно развиваются технологии передачи голосовой информации в режиме реального времени. Системы VoIP (Voice over IP) позволяют осуществлять голосовую связь через интернет-протоколы [10, с. 304], что существенно расширяет возможности пользователей и снижает затраты на коммуникации. При этом важным аспектом является обеспечение качества передачи в условиях различных сетевых задержек и потерь пакетов.

Современные технологии обработки голосовой информации в мобильных сетях достигли значительного прогресса, однако их развитие сопровождается комплексом технических и нормативных вызовов. Алгоритмы сжатия, такие как G.711 и G.729, обеспечивают баланс между качеством передачи и эффективным использованием пропускной способности каналов, но требуют адаптивного подхода для минимизации артефактов. Критически важным остается вопрос безопасности: протоколы SRTP и ZRTP, основанные на динамическом шифровании

и аутентификации, формируют основу защиты данных от перехвата, хотя их реализация зависит от совместимости инфраструктуры.

Интеграция биометрических методов, включая голосовую аутентификацию, повышает надежность систем, но требует строгого соблюдения регуляторных требований, таких как GDPR, особенно при обработке персональных данных в облачных средах. Развитие адаптивных технологий, таких как динамическая модуляция и машинное обучение, позволяет оптимизировать качество связи в условиях нестабильных сетей, а также внедрять предиктивную аналитику для управления ресурсами.

Стандартизация, включая рекомендации ITU-T P.863 для оценки качества голосовых сервисов, остается ключевым фактором обеспечения совместимости и надежности телекоммуникационных систем [3, с. 19–25]. При этом энергоэффективность устройств, достигаемая за счет специализированных процессоров и алгоритмов DRX, критически важна для продления автономности мобильных решений.

Перспективным направлением является интеграция VoIP с искусственным интеллектом, позволяющая не только улучшить качество связи через подавление шумов, но и реализовать эмоциональный анализ речи для персонализированных сервисов. Однако успех дальнейшего развития зависит от межотраслевого сотрудничества, учитывающего этические аспекты использования голосовых данных и ужесточающиеся законодательные рамки.

Список литературы

1. Агеев С. В. Цифровая обработка сигналов в телекоммуникационных системах / С. В. Агеев, В. В. Бутенко, В. Н. Гордиенко. – М.: Горячая линия-Телеком, 2023. – 384 с.
2. Антонов О. Ю. Тактика получения и использования криминалистически значимой информации от операторов связи // Российский следователь. 2020. № 4. С. 3–7.
3. Антонов О. Ю. Взаимодействие с интернет-провайдером в целях собирания цифровых следов // Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: мат-лы науч.-практ. конф. с междунар. участием. М., 2019. С. 19–25.
4. Гольцов С. Е. Процессуальные средства получения доказательств, содержащих голосовую информацию в абонентских устройствах // Теория и практика расследования преступлений: материалы XI Междунар. науч.-практ. конф. Краснодар, 13 апреля 2023 г. Краснодар: Краснодарский ун-т МВД России, 2023. С. 373–377.
5. Гольцов С. Е. Уголовно-процессуальный порядок получения голосовой информации у операторов связи и организаторов распространения информации в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2023. № 3 (27). С. 41–49.

6. Антонов О. Ю. Принципы получения информации о соединениях между абонентами и (или) абонентскими устройствами // Вестник Воронежского государственного университета. Сер. Право. 2021. № 1 (44). С. 239–246.

7. Гаврилин Ю. В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях: науч.-практ. пособие. М.: Академия управления МВД России, 2021. – 71 с.

8. Гаврилин Ю. В., Шипилов В. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 23. С. 3–6.

9. Гаврилин Ю. В., Балашова А. А. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 129–137.

10. Куликов А. С. Методы и средства криптографической защиты информации / А. С. Куликов. – М.: Академия, 2023. – 304 с.

11. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

12. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

13. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

14. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

15. Константинов, А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.

16. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

Зайчикова Г. А.¹,

*командир отделения института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Михайленко Н. М.,

*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

СОВРЕМЕННЫЕ КИБЕРУГРОЗЫ И ИХ ВЛИЯНИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

Критическая информационная инфраструктура (КИИ) – это совокупность систем, сетей и объектов, которые играют критическую роль в обеспечении жизненно важных функций и услуг в современном обществе. Эти функции и услуги включают в себя энергоснабжение, водоснабжение, транспортные системы, здравоохранение, банковские и финансовые услуги, государственное управление, связь и другие ключевые секторы. Современные киберугрозы становятся все более изощренными, масштабными и непредсказуемыми. Используемые злоумышленниками технологии позволяют осуществлять целенаправленные атаки, наносящие значительный вред КИИ. Поэтому для защиты от кибератак требуется не только техническая и правовая, но и политической готовности государств к реагированию на подобные вызовы.

В период с 2024 по 2025 гг. характеризуется значительным ростом и разнообразием кибератак на объекты КИИ.

По информации «Ростелекома», в 2024 г. число зафиксированных атак на КИИ выросло более чем на 80 % по сравнению с 2023 г. Чаще всего использовались целевые шифровальщики (вымогатели), внедряемые через фишинговые письма и эксплойты уязвимостей в ПО.

Вице-президент по развитию и обеспечению информационной безопасности «Ростелекома» Алексей Чугунов отметил следующее: «В “Ростелекоме” мы ежедневно сталкиваемся с новыми киберугрозами, и каждая из атак на нашу инфраструктуру отличается по сложности и продолжительности. Наша экосистема включает множество продуктов, которые вызывают повышенный интерес у злоумышленников. Для эффективной защиты от киберугроз важно регулярно обучать сотрудников, контролировать периметр инфраструктуры, поддерживать ИТ-системы в актуальном состоянии через инвентаризацию и обновления программного обеспечения, а также внедрять и эффективно использовать многоуровневые системы защиты, средства мониторинга и реагирова-

¹ © Зайчикова Г. А., 2025.

ния на инциденты информационной безопасности. Регулярное резервное копирование данных и проведение киберучений помогут минимизировать потери в случае атаки» [1].

Работу эксплойтов можно отразить следующим образом:

1. Находится уязвимая система (например, с открытым RDP (удаленный доступ к компьютеру), чаще всего это происходит из-за слабых паролей, открытых портов или устаревшей версии Windows/Office.

2. Через обнаруженную уязвимую систему загружается вредоносный скрипт или программа.

3. Злоумышленник получает доступ, устанавливает вымогатель и шифрует файлы.

Наиболее популярные и известные целевые шифровальщики в настоящее время можно представить следующим образом (таблица 1).

Таблица 1.

Название	Методы распространения	Особенности
Dharma (также известен как CrySIS и Wadhrama)	Распространялся через поддельные установочные файлы программного обеспечения или фишинговые электронные письма	Добавляет к зашифрованным файлам уникальные расширения, часто включающие ID жертвы и email злоумышленника. Основная цель – зашифровать файлы жертвы, сделав их недоступными, а затем потребовать выкуп за восстановление файлов
Defray777	Распространялся через фишинговые электронные письма, содержащие вредоносные документы Microsoft или использующие уязвимости программного обеспечения	Используется в целевых атаках на крупные компании, больницы, госструктуры. Она попадает на компьютер через сообщения, которые практически неотличимы от официальных, но содержат вредоносные вложения или ссылки. После запуска вредоносного кода чаще всего происходит нарушение работы систем и серверов
Ryuk	Распространяется через вредоносные макросы в фишинговых документах, сторонние вредоносные	Используется в целевых атаках на крупные компании, СМИ, больницы, образовательные организации и госструктуры. Жертве присыла-

	программы и техники эксплойтов	ется вредоносное письмо с зараженными вложениями. Посредством чего злоумышленники получают доступ к внутренней сети, где шифруются все важные данные, включая сетевые ресурсы и резервные копии
Zeppelin	Распространяется через слабые RDP-серверы, вредоносную веб-рекламу и фишинговые письма с вредоносными макросами	Используется в целевых атаках на систему здравоохранения и образования, бизнес и IT сферу. Через фишинговые письма или зараженную онлайн-рекламу, которая автоматически загружает вредоносный код, злоумышленники подбирают пароли или используют украденные учетные записи. Полученные ресурсы используются для шифровки баз данных, удаления теневых копий файлов для обеспечения невозможности восстановления украденной информации

В феврале 2025 г. сообщалось, что российский малый и средний бизнес столкнулся с новой и еще плохо изученной киберугрозой - программой-**вымогателем PE32**.

Шифровальщик проникает через скомпрометированные службы удаленного доступа и, в отличие от большинства шифровальщиков, не похищает данные жертв, а взаимодействие с пострадавшими ведет через электронную почту и Telegram.

По данным «Ростелеком-Солар», в 2024 г. были выявлены атаки на систему документооборота, встроенную в крупные министерства РФ. Злоумышленники внедрили вредоносный код через автоматическое обновление [2].

Организации в КИИ подверглись атакам через зараженные обновления программных продуктов, в том числе отечественного происхождения.

После установки таких обновлений на системах организаций КИИ злоумышленники получали возможность несанкционированного доступа к критически важной инфраструктуре. Эти инциденты подчеркнули необходимость усиления контроля за безопасностью цепочек поставок и проверки подлинности обновлений программного обеспечения.

Для минимизации рисков, связанных с атаками на цепочки поставок, особенно через зараженные обновления программного обеспечения, следует придерживаться следующих рекомендаций:

1. Проводить тщательный аудит безопасности поставщиков и подрядчиков, особенно тех, кто предоставляет программное обеспечение или услуги для КИИ.
2. Внедрять строгие процедуры проверки и валидации обновлений программного обеспечения перед их развертыванием в критически важных системах.
3. Использовать механизмы контроля целостности и цифровые подписи для подтверждения подлинности и неизменности, получаемых обновлений.
4. Обеспечить сегментацию сети и ограничение прав доступа для минимизации потенциального ущерба в случае компрометации отдельных компонентов системы.

Также в 2024 г. фиксировались попытки вывода из строя систем управления тепловыми и гидроэлектростанциями, а также атак на центры обработки данных. По данным ФСБ России, в ноябре 2024 г. предотвращена DDoS-атака на центральную платформу «Цифровой профиль» с попыткой перегрузить удостоверяющие центры. Роскомнадзор в свою очередь сообщил о массовых DDoS-атаках на операторов сотовой связи. «В минувшие выходные были зафиксированы массированные DDoS-атаки, направленные на каналы связи и инфраструктуру нескольких операторов связи, а также на системы крупного хостинг-провайдера. Наибольшая мощность атаки достигала показателя 1,73 Тбит/с», – говорится в официальном заявлении центра [3].

Были совершены многочисленные атаки на госслужащих и сотрудников госкорпораций. Массовая кампания с вредоносным приложением, замаскированным под «Госуслуги», «Госуслуги.Бизнес», а также «ЕМИАС», «МЧС», «Минтруд» и др. Заражение происходило через APK-файлы в сторонних Telegram-каналах. Целью данной кампании было кража персональных данных, отслеживание помещений, а также возможность доступа к корпоративным VPN. Для недопущения таких атак необходимо запретить сотрудникам использовать неофициальные приложения, обеспечить контроль за корпоративными мобильными устройствами, а также отключить возможность установки сторонних APK.

В конце февраля 2025 г. Федеральная служба по техническому и экспортному контролю в лице *Торбенко Елены Борисовны* заявила, что операционные системы на базе AOSP (Android Open Source Project) создают угрозы безопасности для использования в государственных компаниях и на объектах КИИ: «применение AOSP на объектах КИИ создает предпосылки к реализации угроз безопасности информации» [4].

Таким образом, можно увидеть, что киберугрозы способны оказать разрушительное воздействие на критическую информационную инфраструктуру.

В случае кибератаки на банковский сектор или энергетическую систему последствия могут выразиться в миллиардных убытках (простой производств, остановка операций и т. д.). Атаки на системы здравоохранения, водоснабжения или связи могут напрямую угрожать жизни и здоровью граждан. Вмешательство в избирательные процессы, распространение дезинформации и кража политически значимой информации могут дестабилизировать политическую ситуацию в

стране. Атаки на военные системы, объекты стратегического значения или коммуникационные каналы между государственными структурами могут поставить под угрозу обороноспособность страны.

Современные киберугрозы представляют собой одну из наиболее сложных проблем цифровой эпохи. Их влияние на критическую информационную инфраструктуру способно нарушить нормальное функционирование целых государств. В условиях нарастающих цифровых вызовов необходимо консолидировать усилия на национальном и международном уровнях, развивать технологии защиты и формировать культуру кибербезопасности. Важным шагом также является разработка национальных стратегий кибербезопасности [5]. Все эти факторы в совокупности помогут обеспечить устойчивость и безопасность критически важных систем в современном мире.

Список литературы

1. «Ростелеком» отразил более 1 300 кибератак в третьем квартале 2024 года // CYBER MEDIA URL: <https://securitymedia.org/news/rostelekom-otrazil-bolee-1-300-kiberatak-v-tretem-kvartale-2024-goda.html> (дата обращения: 13.04.2025).
2. Ключевые уязвимости информационных систем российских компаний в 2024 году // SOLAR URL: <https://rt-solar.ru/analytics/reports/5375/> (дата обращения: 12.04.2025).
3. Роскомнадзор сообщил о масштабных DDoS-атаках на операторов связи // Ридус URL: <https://www.ridus.ru/roskomnadzor-soobshil-o-masshtabnyh-ddos-atakah-na-operatorov-svyazi-481389.html> (дата обращения: 15.04.2025).
4. 2025: ФСТЭК сообщила, что ОС Android нельзя использовать в критической инфраструктуре // TADVISER. URL: https://www.tadviser.ru/index.php/Статья:Безопасность_Android#.2A_2025:_D0.A4.D0.A1.D0.A2.D0.AD.D0.9A_.D1.81.D0.BE.D0.BE.D0.B1.D1.89.D0.B8.D0.BB.D0.B0.2C_.D1.87.D1.82.D0.BE_.D0.9E.D0.A1_Android_.D0.BD.D0.B5.D0.BB.D1.8C.D0.B7.D1.8F_.D0.B8.D1.81.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D1.82.D1.8C_.D0.B2_.D0.BA.D1.80.D0.B8.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.BE.D0.B9_.D0.B8.D0.BD.D1.84.D1.80.D0.B0.D1.81.D1.82.D1.80.D1.83.D0.BA.D1.82.D1.83.D1.80.D0.B5 (дата обращения: 13.04.2025).
5. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ // Собрание законодательства Российской Федерации.
6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
7. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

8. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
9. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
10. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.
11. Константинов А.В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.
12. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Иванова К. Д.¹,

*командир отделения института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Рудин А. В.,

*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ОСОБЕННОСТИ ВЛИЯНИЯ СМИ И МАСС-МЕДИА НА ФОРМИРОВАНИЕ МАССОВОГО СОЗНАНИЯ

Изучению проблем, связанных с функционированием СМИ, их влиянием на формирование общественного мнения, общественного сознания, сегодня уделяют внимание такие ученые, как Л. Городенко, А. Гриценко, Г. Почепцов, Л. Погорелая и другие.

Говоря о сущности СМИ и масс-медиа, необходимо отметить, что они должны нести в общественную жизнь очень важную функцию – преподносить объективную информацию в «чистом» виде, поднимать социальные проблемы, обращая внимание не только общественности, но и представителей высших государственных органов, давать возможность свободно и открыто выражать мнение граждан в ходе интервью и т. д. Таким образом, СМИ являются своего рода посредниками между личностью (или какой-либо социальной группы) и властью.

В своем исследовании Буркова Л. В. приходит к выводу, что «глобальная информатизация оказывает двойственное влияние на массовое сознание: как позитивное (большая открытость информации для массового сознания, свобода самовыражения и пр.), так и негативное (наличие информационного шума, отсутствие четких критериев для определения надежности источника информации и пр.)» [1].

Говоря о воздействии СМИ и масс-медиа на массовое сознание в своем исследовании, мы считаем необходимым выяснить особенности и характеристики самого субъекта такого влияния. Важно отметить, что медиа выступает не только в качестве информационного ресурса, но и в качестве среды нахождения человека. «Медиасреда – это то, что окружает человека, а также он сам, включенный в медиасреду» [2]. Часто в качестве синонима понятия «медиасреда» употребляют понятие «медиафера». Под медиаферой понимается «часть ноосферы, в которой хранятся различные информационные сущности и ждут, когда появится субъект и начнет их использовать: декодировать, интерпретировать, присваивать». Таким образом, медиафера превращается в управляемую медиасреду только при условии медиаактивности человека. Для более строгой с научной

¹ © Иванова К. Д., 2025.

точки зрения структуры медиа, для этого обратимся к этимологии. Медиа (от лат. «media» – средства, посредники, мн. число от «medium» – середина, среднее число, посредник).

Согласно словарю, «Латинские философские термины», еще Фома Аквинский рассматривал две вещи, имеющие отношение к опосредованию, а именно, причина, почему это называется медиумом, и сам акт посредничества. «Вещь называется средней, потому что она расположена между двумя крайностями (экстремумами), акт медиума – связать крайности. Среднее число может быть физическим, как в движении и изменении; или логическим, когда крайности доказываются силлогистически путем приведения к среднему члену; или морально, когда добродетель является серединой между крайностями порока».

Английское «media» является сокращением от «media of communication(s)», что означает на русском языке «средства коммуникации». Английское «media» может быть также сокращением от «media of mass communication(s)», что означает, соответственно, «средства массовой коммуникации». Жилавская И. В. в своем исследовании в качестве критерия классификации медиа является исторический критерий. Так, согласно этому критерию, все виды средств коммуникации делятся на:

- «прамедиа»;
- рукописные медиа;
- печатные медиа;
- электронные медиа;
- цифровые медиа;
- интегрированные медиа».

В литературе, посвященной изучению сущности и специфики работы медиа, существует также такое понятие, как «медиасистема». В российской науке пристальное внимание к медиасистеме проявил М. В. Шкондин, который рассматривает ее как сложную экономическую, социальную и профессиональную систему, обладающую целостностью совокупности компонентов, выступающих как ее подсистемы (которые могут именоваться также как организованные части, сектора медиасистемы) [3].

На сегодняшний день структурные элементы современных медиасистем остаются все еще не до конца изученными, а потому требуют к себе особого внимания со стороны отечественных ученых. Структура медиасистем включает различные секторы, в которых в свою очередь представлены отдельные структурные элементы. В своих исследованиях Кононова Е. И. выделяет следующие секторы медиасистемы:

- 1) периодическая печать: газеты, журналы;
- 2) радио: национальное, международное;
- 3) телевидение: эфирные телеканалы; кабельные системы ТВ; спутниковое ТВ; телевещание через мобильную телефонию;
- 4) онлайн-медиа: автономные онлайн-медиа, интернет-версии газет, журналов, радио- и телестанций, информационных агентств (сайты, порталы), телеканалы на youtube и других видеохостингах, конвергированные медиа;

5) онлайн-новые социальные медиа: сайты и блоги пользователей, социальные сети.

Необходимо отметить, что разные секторы медиасистем влияют не только на формат и доступность информации, но и на саму природу взаимодействия между медиапроизводителями и аудиторией. Всевозрастающее влияние социальных сетей и платформ требует пересмотра традиционных подходов к исследованию медиа.

Необходимо рассмотреть, как эти новые модели воздействия формируют общественное мнение, каковы их экономические и культурные последствия, и какую роль играет алгоритмическое определение контента. Существующие теории и концепции, выработанные для анализа классических масс-медиа, нуждаются в дальнейшей адаптации и уточнении. Поэтому обращение к структурным изменениям и их диалектики становится не просто актуальным, но и необходимым для глубокого понимания динамики современного медиаландшафта.

Что касается положительного влияния СМИ на массовое сознание, то здесь мы отметим следующие признаки такого влияния. Во-первых, СМИ играют важную роль в формировании общественного мнения по отношению к различным политическим, культурным и социальным событиям (международным и внутригосударственным). Это, в свою очередь, способствует повышению уровня осведомленности населения о важных политических процессах, происходящих внутри страны, что непосредственно влияет на гражданско-правовую позицию личности и общества в целом.

Во-вторых, позитивное влияние СМИ проявляется в их способности формировать содействовать прогрессивным изменениям в законодательстве. Чрезвычайно важным является освещение тем, связанных с правами человека, экологическими проблемами и вопросами здоровья, что способствует формированию ответственного и сознательного общества.

Также стоит отметить, что разнообразие медиаформатов позволяет людям получать информацию в удобной для них форме, что расширяет доступ к знаниям и образовательным ресурсам. Наконец, социальные сети и другие цифровые платформы создают новые возможности для обсуждения, обмена мнениями и налаживания диалога между различными группами населения, что формирует более сплоченное общество.

Подводя итоги, мы можем сказать, что СМИ и масс-медиа являются одними из ключевых информационных ресурсов, с которыми социум сталкивается ежедневно на протяжении всей своей жизни. Именно поэтому нельзя недооценивать огромное влияние данных структур на сознание личности и общества. На сегодняшний день, в век информационных технологий, медиасфера получила свое максимальное развитие за последние десятилетия. Однако, многие скрытые механизмы ее работы и влияния на мозговую деятельность и сознание до сих пор до конца не изучены. Видится целесообразным, расширить данное исследование, привлекая специалистов из таких научных сфер, как психология, нейропсихология и т. д. Дальнейшие исследования в данной области должны быть направлены на изучение конкретных механизмов влияния различных типов медиаконтента на

различные группы населения, а также на разработку эффективных методов повышения медиаграмотности и развития критического мышления в условиях быстро меняющегося информационного пространства. Только комплексный подход, сочетающий в себе научные исследования, образовательные программы и государственную политику в сфере медиа, позволит обеспечить формирование здорового и устойчивого массового сознания, способного успешно адаптироваться к вызовам современного мира.

Список литературы

1. Буркова Л. В. Влияние глобальной информатизации на массовое сознание // Современные философские исследования. № 2. 2018. С. 1–6.
2. Жилавская И. В. Классификация медиа. Проблемы, понятия, критерии // Вестник ВУиТ. 2016. №4. С. 1–7.
3. Кононова Е. И., Короченский А. П. К вопросу о классификации современных медиасистем // Вопросы журналистики, педагогики, языкознания. 2023. №3. С. 1–6.
4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // Российской газета. 2006. № 165.
5. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
7. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
8. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с.
9. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
10. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPYUOY.
11. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

Ивлев К. А.¹,
командир отделения
института подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
заместитель начальника кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

МЕТОДЫ ЦИФРОВОЙ КРИМИНАЛИСТИКИ В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Современные методы цифровой криминалистики стали неотъемлемым инструментом в деятельности правоохранительных органов, трансформируя традиционную криминалистическую методику.

Актуальность темы обусловлена ростом сложности преступлений и необходимостью оперативного сбора доказательств в условиях цифровой эпохи. По данным исследований, внедрение методов цифровой криминалистики в следственную практику позволяет сократить время расследования на 20–30 %, а точность реконструкции событий повышается до 95 % при использовании 3D-моделирования. Однако, несмотря на технологический прогресс, в 2024 г. лишь 45 % следственных подразделений в России применяют современные технологии. Это связано с недостатком финансирования, отсутствием единых стандартов и низким уровнем цифровой грамотности сотрудников [6].

Намереваясь раскрыть преступление по горячим следам, необходимо понимать, что это возможно лишь за счет своевременного проведения необходимых действий, операций, которые зачастую выполняются по «старым» методикам, основанным на «ручных» технологиях. Очевидно, что в ситуации, когда имеется возможность решить одну и ту же задачу также эффективно и в более короткие сроки за счет прогрессивных технологий, использование старых методик становится нецелесообразным.

Одним из способов, способных значительно ускорить решение поставленных задач, следует признать использование возможностей современных информационно-телекоммуникационных систем, стремительно развивающимся благодаря совершенствующимся методам цифровой криминалистики [4].

Технологии искусственного интеллекта трансформируют анализ собранных данных. Алгоритмы машинного обучения выявляют микрочастицы, изменения

¹ © Ивлев К. А., 2025.

структуры поверхностей или аномалии в распределении следов, которые не фиксируются человеческим глазом. В Дальневосточном федеральном округе внедрение платформ с искусственным интеллектом сократило время обработки материалов на 40% за счет автоматической классификации доказательств и их привязки к базе данных ДНК. Однако эффективность таких систем напрямую зависит от качества обучающих выборок. Известны случаи, когда предвзятость алгоритмов приводила к ошибкам в идентификации лиц из этнических меньшинств, что подчеркивает необходимость этического аудита ИИ-решений [6].

Фотограмметрические методы, основанные на компьютерной обработке снимков, обеспечивают не только высокую точность измерений, но и возможность реконструкции динамики событий. Например, при расследовании убийств 3D-моделирование помогает восстановить последовательность ударов, определить угол атаки или положение жертвы в момент нападения. Технология сферических фотопанорам, интегрированная в программные комплексы типа «ФОМП-К», позволяет создавать интерактивные туры по месту происшествия, что упрощает проверку показаний свидетелей. При этом обработка данных требует ручной корректировки из-за возможных искажений в автоматическом построении моделей, что увеличивает трудоемкость процесса [6].

Перспективным направлением является интеграция методов цифровой криминалистики в судебные процессы. Программы типа 3D EyeWitness позволяют создавать анимированные реконструкции преступлений, демонстрируя действия подсудимых в зале суда. Это не только повышает наглядность, но и снижает субъективность восприятия доказательств присяжными. Однако такие технологии требуют адаптации уголовно-процессуального законодательства, особенно в части допустимости цифровых доказательств [4].

В связи с этим необходимо сделать вывод модернизации законодательной базы. Введение понятия «цифровое доказательство» в УПК РФ позволит легализовать использование 3D-моделей, данных ИИ-анализа и материалов, полученных с помощью БПЛА. Это требует разработки стандартов фиксации и хранения таких доказательств, а также их интеграции в единую межведомственную платформу. Подобная платформа могла бы объединить криминалистические учеты, биометрические системы и записи камер наблюдения, но ее создание потребует пересмотра норм о защите персональных данных и межведомственном взаимодействии [4].

Однако внедрение инноваций сталкивается с организационными и правовыми барьерами. Неравномерная техническая оснащенность регионов приводит к тому, что современные методы остаются недоступными для значительной части следственных подразделений. Низкий уровень цифровой грамотности сотрудников усугубляет ситуацию: даже при наличии оборудования его использование зачастую ограничивается из-за недостатка компетенций. Отдельной проблемой остается фрагментация данных между ведомствами.

Этические риски, связанные с применением искусственного интеллекта, требуют особого внимания. Непрозрачность алгоритмов, риски дискриминации при идентификации лиц и утечки персональных данных создают угрозы для прав

граждан. Отсутствие механизмов этического аудита технологий повышает вероятность ошибок, которые могут повлиять на исход судебных процессов.

Для преодоления этих проблем необходим комплексный подход. Первостепенным направлением является модернизация инфраструктуры: обеспечение регионов оборудованием, создание единых платформ для хранения и анализа данных, а также разработка стандартов использования современных методов цифровой криминалистики.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921.
2. Применение 3D-моделирования в криминалистике: опыт Германии // Криминалистический вестник. – 2010. – № 3. – С. 45–50.
3. FARO Focus Premium [Электронный ресурс]. – Официальный сайт FARO Technologies. – URL: <https://www.faro.com> (дата обращения: 25.02.2025).
4. 3D EyeWitness: программное обеспечение для реконструкции преступлений [Электронный ресурс]. – URL: <https://www.3deyewitness.com> (дата обращения: 25.02.2025).
5. Европейская этическая хартия по искусственному интеллекту [Электронный ресурс]. – Совет Европы, 2018. – URL: <https://www.coe.int/en/web/artificial-intelligence/ethics-charter> (дата обращения: 25.02.2025).
6. О состоянии технической оснащенности следственных подразделений в 2024 году: отчет МВД России. – М., 2024.
7. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.
8. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
9. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
10. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
11. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
12. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва

: Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

13. The Adversarial Approach in the Pretrial Phase of Prosecution / V. V. Pushkarev, E. A. Trishkina, E. V. Tokareva [et al.] // Cuestiones Políticas. – 2020. – Vol. 37, No. 65. – P. 281–287.

Каргин Н. М.¹,
 курсант института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Токолов А. В.,
 доцент кафедры противодействия преступлениям
 в сфере информационно-телекоммуникационных технологий
 Московского университета МВД России имени В.Я. Кикотя,
 кандидат юридических наук

ОСОБЕННОСТИ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ В СФЕРЕ ФИНАНСОВ

На сегодняшний день существует значительное количество научных работ, посвященных изучению противоправных деяний, совершаемых посредством компьютерных либо иных цифровых инструментов. В указанных исследованиях применяются достаточно широкие дефиниции, позволяющие включить в сферу анализа разнообразные правовые конструкции и материальные объекты. Современная юридическая наука активно применяет термины вроде «электронные системы обработки данных», «автоматизированные информационные процессы», «современные цифровые решения», «интернет-ресурсы» для описания рассматриваемых правонарушений, зачастую трактуя данные понятия как взаимозаменяемые. Например, В. В. Хилюта обращает внимание: «...на то обстоятельство, что действующие уголовно-правовые нормы (преступления против собственности) сориентированы исключительно на охрану вещей и меньшей степени направлены на уголовно-правовую охрану имущественных прав и оборот экономических благ» [1], и в результате научных исследований им предлагается учение о преступлении против оборота объектов гражданских прав, в число которых войдут и киберпреступления в финансовой сфере. Так, по мнению, Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинова: «...следует обратить внимание, что в предварительных материалах Конгресса (Конгресс ООН 20–27 апреля 2020 г. в г. Киото – прим. автора) понятия «киберпреступность», «компьютер» уже практически не используются. Речь идет о современных информационных и цифровых технологиях» [2]. Данными авторами отмечается широта понятия «цифровая преступность» в соотношении с понятием «киберпреступность». Например, И. Б. Ардашкин пишет: «Смарттехнологии – это понятие, которым сегодня различные авторы стремятся обозначить самые современные технологические разработки. ...Они имеют также большое количество похожих наименований (конвергентные технологии, NBIC (NBICS) – технологии, информационные технологии, информационно-

¹ © Каргин Н. М., 2025.

коммуникационные информации, цифровые технологии и т.д.)» [3]. По мнению В. И. Гриценко и Б. Н. Паньшина информационные технологии «это информационные процессы, реализуемые в многомашинных комплексах, локальных и распределенных сетях ЭВМ» [4]. П. Д. Белашов и И. С. Разуваев говорят, что «компьютерные технологии — часть информационных технологий, которая основывается на применении компьютеров, активном участии пользователей (непрофессионалов в области программирования) в информационном процессе, высоком уровне дружественного пользовательского интерфейса, широком использовании пакетов прикладных программ общего и проблемного назначения, доступе пользователя к удаленным базам данных и программ благодаря вычислительным сетям ЭВМ» [5].

В соответствии с определениями информационных технологий, прописанными в современных регулирующих документах, таких как Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, ГОСТ 34.033-90, ISO/IEC 38500:2015 — можно заключить, что эти технологии охватывают весь спектр как вычислительных механизмов, так и самих вычислительных ресурсов. История термина «киберпреступность» прошла через трансформации, которые были отслежены Я. Г. Ищуком, Т. В. Пинкевичем и Е. С. Смольяниновым, и претерпевала постепенные изменения на протяжении 70-80-х гг. XX в., а затем совершенствовалась и переходила в цифровую форму в 2000, 2005 и 2020 гг. на крупных форумах ООН. С точки зрения технических характеристик цифровые технологии основаны на дискретизации сигналов аналоговых уровней и содержат логические элементы (AND, OR, NOT и т. д.), связанные счетчиками или триггерами. Исходя из данной позиции, представители социально-гуманитарных наук обязаны учитывать фактическое содержание обозначений, связанных с современными технологиями. По моему убеждению, разделение понятий «киберпреступление» и использование современных информационных ресурсов как средства совершения преступления представляется необоснованным, поскольку подавляющее большинство киберугроз реализуется именно посредством цифровых каналов связи. С. А. Петров отмечает: «Преступник не сам тайно изымает эти деньги, а компьютер, банкомат, другое электронное устройство передают их ему внешне добровольно, но в связи с ошибкой в программе, которую сознательно вносит в эту программу виновный» [6]. Преднамеренное внесение изменений в работу программного обеспечения, с целью украсть деньги или конфиденциальные данные, которые можно конвертировать, свидетельствует о намерении совершить киберпреступления в финансовой области. Проводя анализ уголовных дел, О. М. Иванова пишет: «Как видно из материалов уголовных дел, хищения чужого имущества, в особенности многоэпизодные, совершаются чаще всего с заранее обдуманым умыслом. Безусловно, данная разновидность умысла особенно характерна для замаскированных хищений» [7]. На настоящий момент преобладает тенденция квалификации большинства случаев финансовых киберпреступлений исключительно как тайного похищения чужого имущества, регулирующегося положениями ст. 158 Уголовного кодекса Российской Федерации. Лично убежден, что субъективная сторона каждого такого правонарушения характеризуется наличием прямого умысла, однако ситуация

существенно усложняется, когда программное обеспечение разработано специально для атаки на информационную инфраструктуру банков и кредитных организаций, но не применяется самим создателем, а передается третьим лицам. Подобные деяния будут квалифицироваться уже по другим основаниям, предусмотренным ст. 273 УК РФ, и никак не связаны с совершением хищения, причем сфера возможного использования вредоносного продукта не ограничивается финансовыми учреждениями и может затрагивать любые отрасли экономики и социальной сферы. Такого рода действия фактически подпадают под признаки открытой формы хищения, регулируемой нормами ст. 161 УК РФ. Примером служит известная группа *Visness Club*, осуществлявшая масштабные нападения на американские банковские структуры путем вывода средств со счетов, сопровождаемого всплывающим сообщением об ошибке на экранах банковских терминалов, блокирующим возможность персонала вмешаться в ситуацию.

На мой взгляд, особый акцент следует сделать на конспиративный характер киберпреступлений в финансовой сфере, поскольку именно эта черта способствует значительному росту числа подобных правонарушений и затрудняет борьбу с ними. Научные труды специалистов В. А. Номоконова и Т. Л. Тропиной выделяют ряд уникальных особенностей, присущих финансово направленным киберпреступлениям, которые резко контрастируют с иными видами нарушений законодательства. Полностью солидаризируюсь с представленными выводами ученых и настаиваю на необходимости тщательного изучения и дальнейшего осмысления характеристик данного типа преступлений. Уже в 2011 г. исследователь С. М. Иншаков провел детальное исследование уровня латентности киберпреступлений, выявив следующие показатели: по ст. 272 УК РФ коэффициент составил 4,8; ст. 273 УК РФ – 11,8; ст. 274 УК РФ – около 30 единиц. Данный аспект получил подтверждение и в международных источниках: Обзор Исполнительного комитета Содружества Независимых Государств «Некоторые правовые аспекты противодействия киберпреступности в государствах-членах СНГ» (2014 г.) констатирует высокую степень сокрытости киберпреступлений: уровень латентности достигает примерно 80 % в Соединенных Штатах Америки, до 85 % в Соединенном Королевстве, порядка 75 % в Федеративной Республике Германия и превышает отметку в 90 % в Российской Федерации.

По утверждению авторитетного ученого А. Э. Побегайло, зафиксированная в 2018 г. общая тенденция высокого уровня латентности финансово мотивированной киберпреступности сохраняется и поныне, что находит свое отражение и в трудах другого исследователя – А. С. Лакова. Это явление обусловлено преимущественно технологическими факторами: перемещение по сетевым сегментам злоумышленники осуществляют посредством стандартного программного обеспечения и штатных возможностей операционных систем, широко используемых в организациях. Операция копирования исполняемого файла *Isass.exe* и последующего перехвата аутентификационной информации пользователей с помощью специализированной утилиты *mimikatz*, осуществляемая на оборудовании преступника, остается незамеченной, поскольку задействуются легально используемые инструменты для захвата содержимого оперативной памяти и последующего автоматического исполнения. Во избежание фиксации собственного присутствия нарушители нередко

применяют автономно действующий вредоносный код, работающий исключительно в оперативной памяти целевой машины, а также внедряют его в автоматические процессы загрузки операционной системы для долговременного удержания контроля над объектом даже после перезагрузки. Помимо указанного метода сокрытия активности, высокоуровневые кибератаки против инфраструктуры финансовых учреждений включают дополнительную манипуляцию с регистрационными файлами и таблицами разметки накопителей, уничтожающими следовую картину инцидента. Запущенный однажды вредоносный процесс чрезвычайно трудно прекратить. Активизация практики использования злоумышленниками технологий анонимизации трафика (*Tor*, *VPN*-сети, прокси-серверы и др.) существенно усугубляет проблему латентности криминальных проявлений в финансовой киберсфере.

Расследования подобных дел осложнены серьезными международными препятствиями, вызванными межведомственной разобщенностью и политическими конфликтами между государствами, в частности, между Россией и западными странами. Типичным случаем является история международной банды *Carbanak*, выявленная в 2014 г. и состоящая из представителей России, Казахстана и ряда европейских стран. После ареста некоторых фигурантов дела преступная сеть продолжает существовать, сохраняя потенциал для новых атак благодаря уникальным инструментам, позволявшим группе долгие годы контролировать крупные финансовые институты. Авторы исследования «Анатомия киберриска» Р. Джамиллов, Х. Рей и А. Тахун справедливо указывают, что данная проблема носит временной характер и постепенно исчезнет по мере достижения страхового сектора и финансовых технологий высоких стандартов безопасности.

Для успешного совершения киберпреступлений в финансовой сфере, которые направлены на хищение денежных средств, часто требуется провести физическое обналичивание похищенных денег. Для этой цели в масштабных киберпреступлениях использовались дропы – лица местного населения, которые привлекались или специально командировались для снятия денег в банкоматах. Правоохранительные органы обычно задерживают дропов, однако из-за недостаточных знаний о структуре и работы киберпреступной группы, организаторы преступления часто остаются не идентифицированными. В 2013 г. группой экспертов УПН ООН (Управление по преступности и наркотикам ООН) был представлен доклад «Всестороннее исследование проблемы киберпреступности», в котором с осторожностью отмечено: «Многие киберпреступления требуют высокой степени организованности и специализации, и вполне возможно, что степень вовлеченности обычных преступных групп в киберпреступную сферу высока, по крайней мере, в части киберпреступлений, совершенных в целях получения финансовой выгоды, таких как компьютерное мошенничество, подлог и использование персональных данных...» [8]. «Черный рынок» киберпреступности характеризуется степенью взаимодействия групп и частных лиц, выполняющих различные и иногда множественные роли (включая «программистов», «распространителей», «технических специалистов», «хакеров», «мошенников», «хостеров», «обналичивателей средств», «денежных курьеров», «кассиров» и «лидеров») в процессе создания вредоносного программного обеспечения, компьютерного заражения (в частности, посредством фишинга электронной

почты), управления бот-сетями, сбора персональных и финансовых данных, продажи сведений и получения денег за финансовую информацию». Евразийская группа по противодействию легализации незаконно нажитых капиталов и финансирования террористических актов в рамках тематического исследования «Киберпреступность и отмывание денежных средств», проведенного в 2014 г., подчеркнула существенную разницу между традиционным и киберотмыванием капитала. Она отметила, что современный подход включает широкий спектр транзакций и посреднических сервисов, начиная от классических банковских переводов и заканчивая услугами онлайн-платежей, привлечением посредников – «денежных мулов» и альтернативных схем обмена валюты. Следовательно, целесообразно рассматривать киберпреступность в финансовой сфере как гибрид классической экономической преступности и современной киберкриминальной деятельности.

Особое значение приобретает возможность монетизировать промежуточные этапы преступления. Так, получив доступ к IT-инфраструктуре банка, злоумышленник способен продать полученный доступ на теневых ресурсах DarkNet. Цена зависит от репутации пострадавшей организации и глубины проникновения в ее внутреннюю сеть. Именно эта возможность превращает доступ в товар, создавая дополнительный стимул для активных действий киберпреступников.

Тем не менее повторная реализация различных этапов атаки позволяет злоумышленникам повысить ее эффективность и снизить последствия для себя. В некоторых случаях, подготовительный этап киберпреступления может быть рассмотрен как завершенное преступление с использованием ст. 272 УК РФ. Создание точки доступа также может происходить без непосредственного использования ее в преступных целях, однако с умыслом на ее дальнейшую эксплуатацию. В случаях реализации подготовленной точки доступа возможна дополнительная квалификация по ст. 175 УК РФ. Применение положений ст. 175 Уголовного кодекса Российской Федерации в данном конкретном случае видится целесообразным, поскольку формирование нелегальной точки входа в информационно-техническую структуру банковской организации изначально представляет собой нарушение права собственности и связано с заведомой противоправностью таких действий. Вместе с тем современные научные изыскания подтверждают, что нынешняя обстановка кардинально изменилась: если раньше преступные посягательства касались главным образом материальных предметов, то ныне они направлены на интеллектуальные ценности и нематериальные активы, обладающие сопоставимой стоимостью с традиционными вещами. Оценивая состав основного и финального этапов первого и третьего подходов к совершению преступлений в финансовой сфере, мы приходим к выводу о совпадении их юридической оценки, тогда как второй метод подразумевает квалификацию начального этапа по пункту четвертому ст. 159.6 УК РФ, а заключительного – по второму пункту ст. 272 УК РФ, при условии внесения предлагаемых поправок, сформулированных в разделе 1.2 настоящего исследования. В итоге выделились три главных направления АРТ-атак: воздействие на банкоматные сети, проникновение в корпоративные сегменты Банков России и инфицирование персональных рабочих станций для похищения учетных данных. Первая методика оптимальна для атак на коммерческие банки и прочие субъекты рынка фи-

нансовых услуг, располагающиеся владельцами обширных сетей банкоматов, платежных терминалов и прочих аналогичных устройств; вторая направлена исключительно на атаку коммерческих банков; третья схема универсальна и охватывает любой объект в сфере финансов, будучи наименее ресурсоемкой как материально, так и технически. Я увидел некоторые черты киберпреступлений финансового характера, как технические, так и юридические, которые, на мой взгляд, отличают их от других видов преступлений в интернете:

- высокая латентность;
- многоэпизодность;
- наличие финансовой грамотности у преступников либо сговора с сотрудником финансовой организации;
- наследственность технических процессов;
- возможность монетизации промежуточных результатов преступной деятельности; лидирующая роль социальной инженерии как преступного инструментария;
- смещение преступных посягательств с банков на страховые и финтех-компании;
- симбиоз или сращивание финансово-ориентированной киберпреступности и традиционной; умышленный характер.

Список литературы

1. Хилjuta В. В. Преступления против оборота объектов гражданских прав: концептуально-теоретические основы моделирования. Резюме дис. ... д-ра юрид. наук. Минск, 2021. – 63 с.
2. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология: учебное пособие. М.: Академия управления МВД России, 2021. – 244 с.
3. Ардашкин И. Б. Смарт-технологии как феномен: концептуализация подходов и философский анализ. Являются ли смарт-технологии действительно умными? // Вестник Томского государственного ун-та. Философия. Социология. Политология. 2018. № 43. С. 55–68.
4. Гриценко В. И., Паньшин Б. Н. Исходная концепция об определении понятия информационной технологии // Вестник Российского общества информатики и вычислительной техники, 1990. Вып. 2. С. 67–77.
5. Белашов П. Д., Разуваев И. С. Понятие «компьютерные технологии в рамках информационных технологий в обучении». XXI век: итоги прошлого и проблемы настоящего плюс. Пенза: Изд-во: Пензенского государственного технологического ун-та, 2015. Т. 1. № 6 (28). С. 54–60.
6. Петров С. А. Особенности квалификации хищений, совершаемых с использованием компьютерной техники // Российский следователь, 2008. № 15. С. 22–24.
7. Иванова О. М. Хищения чужого имущества как уголовно-правовая категория: дис. ... канд. юрид. наук. Самара, 2020. – 319 с.

8. The Adversarial Approach in the Pretrial Phase of Prosecution / V. V. Pushkarev, E. A. Trishkina, E. V. Tokareva [et al.] // Cuestiones Políticas. – 2020. – Vol. 37, No. 65. – P. 281–287.

9. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

10. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

11. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

12. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

13. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

14. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.

Кеслер П. В.¹,

курсант института

подготовки сотрудников для органов

предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Константинов А. В.,

заместитель начальника кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ СИСТЕМЫ «СОВКОМБАНК» КАК КЛЮЧЕВАЯ СТРАТЕГИЯ ПРЕДОТВРАЩЕНИЯ ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ

В эпоху стремительного роста цифровизации и увеличения количества обрабатываемых данных, вопросы защиты информации становятся первостепенными для финансовых организаций. Поскольку текущие кибернетические опасности характеризуются повышенной сложностью и расширением масштабов, создавая риски не только для непрерывности функционирования банковских систем, но и для конфиденциальности клиентских сведений, то создание и применение действенных стратегий информационной безопасности является ключевой необходимостью для банковского сектора, что и обуславливает высокую актуальность изучения данного вопроса.

Из вышесказанного можно сформулировать, что комплекс мероприятий, ориентированных на охрану информационных активов от неправомерного проникновения, изменения, уничтожения или утраты, представляет собой информационную безопасность. Ключевые принципы данного вида защиты охватывают конфиденциальность, целостность и доступность данных. Конфиденциальность регламентирует предоставление доступа к информации исключительно уполномоченным на то лицам. Второй базис построения безопасности гарантирует защиту данных от несанкционированных корректировок, в то время как третий обеспечивает возможность использования информации в нужный момент времени.

В связи с этим, для поддержания информационной безопасности Совкомбанк как одна из самых быстрорастущих и высокодоходных финансовых групп России реализовал ряд мер: управление правами доступа к информационным платформам, обеспечение отказоустойчивости информационных активов, применение специализированных средств защиты, а также ограничение доступа в Интернет исключительно для служебных целей. С целью исключить несанкционированное

¹ © Кеслер П. В., 2025.

проникновение в офисные помещения он также стал использовать в своей деятельности [1]:

- 1) системы контроля доступа;
- 2) мониторинг посредством видеонаблюдения;
- 3) охранно-пожарную сигнализацию;
- 4) физическую защиту при помощи сейфов и специализированных шкафов.

Принимая во внимание актуальные риски в цифровой среде, методы защиты информации, применяемые Совкомбанком, отвечают современным стандартам. Так, технологические решения, в частности, криптографические алгоритмы и многоуровневая аутентификация, гарантируют повышенную степень защиты. Вместе с тем, существенное количество инцидентов кибернетического характера, направленных против финансовых организаций в 2022 г., достигающее отметки в 25 000 зафиксированных атак, акцентирует внимание на важности регулярной модернизации защитных механизмов.

Необходимо подчеркнуть, что концепции соглашений Российской Федерации рассматривают международную информационную безопасность как состояние международных отношений, способное обеспечить устойчивость и безопасность государств в киберпространстве в глобальном масштабе. Это акцентирует важность комплексного подхода к обеспечению киберзащиты, который охватывает не только технические меры, но и взаимодействие на международном уровне.

Согласно проекту концепции стратегии кибербезопасности в Российской Федерации в основе ее реализации лежат следующие основные принципы [2]:

1. Обеспечение гарантированности конституционных прав и свобод граждан в сфере доступа к информации и пользования ею.
2. Максимальная защита частных лиц и организаций, в том числе тех, кто отвечает за работоспособность критически важной информационной инфраструктуры, а также государственных органов в части защиты их информационных ресурсов, систем и сетей в киберпространстве.
3. Развитие плодотворного взаимодействия между всеми участниками информационного общества – гражданами, организациями и государством – в целях укрепления кибербезопасности.
4. Систематическое обновление инструментов и подходов киберзащиты для обеспечения эффективной борьбы с постоянно изменяющимися кибернетическими угрозами.
5. Приоритетность рисков в сфере кибербезопасности, основанная на оценке вероятности наступления киберугроз и масштаба потенциального ущерба, который может быть нанесен в результате инцидентов, связанных с кибербезопасностью, и др.

Поскольку персональные данные клиентов являются для каждого банка одним из важнейших объектов охраны, то и меры, направленные на их безопасность, должны быть соответствующими.

В соответствии с политикой обработки персональных данных Совкомбанк в процессе взаимодействия с ними руководствуется следующими принципами [3]:

1. Персональные данные подлежат обработке исключительно в той мере, в какой это необходимо для достижения заранее определенных целей. Содержание

и объем обрабатываемой информации должны строго соответствовать заявленным задачам.

2. Не допускается обработка избыточных персональных данных, то есть информации, не имеющей прямого отношения к установленным целям.

3. При обработке обеспечивается достоверность и достаточность персональных данных, а также их своевременное обновление в соответствии с целями обработки.

4. В случае обнаружения неполных или неточных данных, они подлежат уточнению или удалению.

5. Хранение персональных данных осуществляется в формате, позволяющем идентифицировать субъекта данных, в течение периода, не превышающего сроки, необходимые для достижения целей обработки. Исключение составляют случаи, когда федеральным законом или договором, в котором субъект персональных данных выступает стороной, выгодоприобретателем или поручителем, не установлен иной срок хранения.

Для более подробного рассмотрения темы информационной безопасности в концепции Совкомбанка считаю необходимым изучить конкретный пример, который раскроет реализацию мер, нацеленных банком для обеспечения безопасности персональных данных своих клиентов.

В мае 2020 г. в банке был обнаружен сотрудник внешнего колл-центра, который незаконно копировал интернет-заявки, поступающие ему для обзвона от лидогенераторов. В ходе следственных действий было выяснено, что данными действиями он намеревался продать скопированные им данные в даркнете. Злоумышленник был арестован сотрудниками органов внутренних дел, но позже освобожден под подписку о невыезде. Копии списков заявок, хранившиеся на жестком диске его компьютера и внешних носителях, были изъяты.

Тем не менее, еще в ходе следствия подозреваемый не оставил попытки прекратить свой преступный умысел, продолжая пытаться реализовывать украденные копии заявок и размещая объявления об их продаже в своем телеграмм-канале, который был связан с его номером мобильного телефона. В связи с этим инцидентом по заявлению Совкомбанка было инициировано уголовное дело в ОМВД по городу Каспийску Республики Дагестан, которое затем было передано в УФСБ России по Республике Дагестан. В настоящее время уголовное дело направлено в суд по ч. 3 ст. 183 и ч. 2 ст. 274.1.

После данного случая первый заместитель председателя правления Совкомбанка Сергей Хотимский отметил: «особый цинизм в том, что повторная попытка мошенничества произошла в момент, когда уже было подано заявление в полицию и активно велись следственные действия. Эта ситуация наглядно демонстрирует излишнюю мягкость российских законов в отношении данного типа преступлений, который активно используется мошенниками. Мы считаем, что российское законодательство по защите информации и коммерческой тайны давно требует ужесточения» [4].

В результате анализа данного события служба информационной безопасности Банка разработала и внедрила комплекс мер, направленных на предотвращение повторения аналогичных ситуаций.

Помимо этого, с 24 июня 2023 г. изменения коснулись и Кодекса Российской Федерации об административных правонарушениях, затрагивающие банки, некредитные финансовые учреждения, государственные компании и ряд других субъектов. Так, в случае передачи платежных документов через мессенджеры, включенные в реестр Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, предусмотрены штрафные санкции:

1) для должностных лиц размер штрафа варьируется от 30 000 до 50 000 рублей;

2) для юридических лиц – от 100 000 до 700 000 рублей.

Аналогичное наказание может быть применено при несоблюдении запрета на подключение сторонних информационных систем к указанным социальным сетям для осуществления безналичных переводов денежных средств граждан Российской Федерации.

Следует отметить, что вышеупомянутым юридическим лицам запрещено использовать мессенджеры из установленного списка при реализации товаров, выполнении работ, оказании услуг и передаче имущественных прав для обмена следующими категориями данных:

- персональные данные граждан Российской Федерации;
- сведения, касающиеся безналичных переводов денежных средств;
- информация, необходимая для осуществления платежей;
- данные о банковских счетах и вкладах граждан России.

В перечень социальных сетей, использование которых для указанных целей запрещено, входят такие платформы, как WhatsApp, Telegram, Skype и Viber.

Мы полагаем, что введение этой меры призвано сократить вероятность несанкционированного доступа к данным о гражданах России за пределами страны. Такая угроза существует в связи с тем, что вычислительные мощности, задействованные в обработке информации, территориально находятся за пределами Российской Федерации.

Федеральная инициатива «Технологии добра», разработанная Совкомбанком совместно с Sk Fintech Hub (Сколково, группа ВЭБ.РФ), предоставляет некоммерческим организациям и благотворительным фондам безвозмездную цифровую помощь в области кибербезопасности. В рамках этой поддержки предлагаются инструменты для обеспечения информационной защиты сотрудников, а также для защиты веб-сайтов от DDoS-атак и вредоносных программ. Однако данные продукты и услуги снабжаются специализированными IT-компаниями, являющимися партнерами проекта.

Так, на платформе «Технологии добра» Совкомбанк и партнеры инициативы обеспечивают некоммерческие организации и благотворительные фонды продуктами и сервисами на безвозмездных или льготных условиях. Помимо этого, проект ориентирован на разработку специализированных цифровых инструментов, адаптированных к нуждам благотворительного сектора.

Лицензированные решения от «Лаборатории Касперского» способствуют обеспечению безопасности рабочих мест: защите компьютеров, файловых серверов и мобильных устройств. Наконец, эксперты компании подберут оптимальное

защитное решение, учитывая индивидуальные потребности и размеры организации.

В настоящий момент свыше 250 некоммерческих организаций и благотворительных фондов активно используют сервисы, представленные на портале «Технологии добра».

Говоря об общих мероприятиях, реализация которых необходима для обеспечения информационной безопасности, как граждан, так и банковской организации, можно отметить следующие. Для граждан: изучение рекомендаций по использованию сложных паролей, двухфакторной аутентификации и обновлению программного обеспечения; использование антивирусных программ и систем обнаружения вторжений. Для банковских организаций: обучение сотрудников стандартам информационной безопасности, включая противодействие социальной инженерии; регулярные тренинги по выявлению мошеннических схем и методам реагирования на инциденты; шифрование данных, как на уровне хранения, так и при передаче, с использованием современных криптографических алгоритмов; внедрение многофакторной аутентификации для доступа к критическим системам и ресурсам.

Подводя итог, необходимо отметить, что перспективы дальнейших исследований данной темы заключаются в разработке более эффективных стратегий интеграции информационной безопасности в деятельность банка, а также в анализе новых технологий, способных повысить уровень защиты данных. Особое внимание следует уделить совершенствованию правовых норм и стандартов, регулирующих информационную безопасность, с учетом специфики финансовой отрасли. Это позволит не только адаптироваться к стремительно изменяющемуся киберугрозам, но и укрепить устойчивость банковской системы в целом.

Список литературы

1. Концепция информационной безопасности // sovcombank.ru URL: https://sovcombank.ru/about/sustainability/policies/kontseptsiya-informatsionnoi-bezopasnosti?ysclid=majmnz2pdm633745090&utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 02.05.2025).
2. Совещание «О разработке стратегии национальной кибербезопасности Российской Федерации: состояние, предпосылки, механизм и перспективы» // council.gov.ru URL: <http://council.gov.ru/events/news/28863/?hl=стратегии%20национальной%20кибербезопасности> (дата обращения: 07.05.2025).
3. Политика обработки персональных данных // sovcombank.ru URL: https://sovcombank.ru/about/pages/policy-personal-data?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 08.05.2025).
4. Утечка из Совкомбанка // securitylab.ru URL: <https://www.securitylab.ru/blog/personal/valerykomarov/351438.php?ysclid=majmpt347k938423130> (дата обращения: 08.05.2025).
5. Инструкция Банка России от 30.05.2014 № 153-И «Об открытии и закрытии банковских счетов, счетов по вкладам, депозитных счетов» // sovcombank.ru

- URL:https://sovcombank.ru/about/pages/policy-personal-data?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 03.05.2025).
6. Марданов Р. Х., Ильин И. В. Стандарты информационной безопасности в банковской системе // Вестник Уфимского государственного авиационного технического университета. 2013. Т. 17. № 7. С. 55–60.
 7. Пушилин В. Эволюция IT-систем влияние на банковский бизнес // Банковские технологии. 2015. № 4.
 8. Положение Центрального банка РФ от 15.10.2015 № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма»; // КонсультантПлюс Надежная правовая поддержка URL: https://www.consultant.ru/document/cons_doc_LAW_190354/ (дата обращения: 05.05.2025).
 9. Сердюк В. Роль стандартов Банка России в обеспечении информационной безопасности кредитно-финансовых организаций // Бухгалтерия и банки. 2008. № 3.
 10. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.
 11. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
 12. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
 13. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
 14. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
 15. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
 16. The Adversarial Approach in the Pretrial Phase of Prosecution / V. V. Pushkarev, E. A. Trishkina, E. V. Tokareva [et al.] // Cuestiones Políticas. – 2020. – Vol. 37, No. 65. – P. 281–287.

Козлова А. В.¹,
*курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Токолов А. В.,
*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ПРОБЛЕМА РАЗВИТИЯ ПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ ДЛЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Различные темы, связанные с информационно-телекоммуникационной сетью, являются актуальными в нынешнее время, поскольку любая деятельность в современном мире так или иначе касается данной сферы. В последние годы ведется активная законодательная деятельность, направленная на урегулирование правоотношение в интернет-сфере. Большая часть принятых нормативных актов была встречена негодованием общественности, так как механизм их реализации заключается в контроле за сетью интернет. Таким образом, в развитии Российской интернет-преступности и мер противодействия ей можно выделить пять основных этапов:

1. 80-90 гг. XX в. – активная подготовка к выходу в глобальную сеть Интернет. Интернет-преступность отсутствует как явление, однако ее возникновение предвидится. Принимаются попытки разработки правовых и организационных средств борьбы с преступлениями в сфере высоких технологий.

2. 7 апреля 1994 г. – рождение Рунета. Первые интернет-преступники начинают свою противоправную деятельность, однако меры борьбы с преступностью России оказались не подготовлены к этому. Продолжаются попытки реформирования законодательства в части ответственности за компьютерные преступления.

3. Июнь 1996 г. – активное внедрение интернета во все сферы жизни общества. Интернет-преступность увеличивает свои количественные и качественные показатели. Создана законодательная база, предусматривающая санкции за совершение компьютерных преступлений, определены требования к защите информации и создано специализированное подразделения по борьбе с преступлениями в сфере высоких технологий.

¹ © Козлова А. В., 2025.

4. 2000 г. – Интернет становится все доступнее. Киберпреступность приобретает глобальный масштаб. Принимается ряд международных актов о борьбе с киберпреступностью, которые Россией не ратифицированы в полном объеме до сих пор. Осуществлено внедрение технических средств борьбы с компьютерными преступниками. Общественность включается в процесс противодействия сетевой преступности.

5. 2011 г. – настоящее время – характеризуется бурным развитием интернет-технологий: совершенствованием имеющихся и появлением новых. Интернет-преступность становится все более общественно – опасной, более изощренной, появляются новые способы и схемы преступной деятельности.

Сегодня организационные и технические средства борьбы с интернет-преступниками остались на уровне IV этапа. В законодательство вносятся отдельные изменения, принимаются новые нормативные и правовые акты, однако они значительно отстают от темпов развития преступности в данной области. Анализ принятого в последние годы законодательства в сфере интернет-отношений дает нам основания полагать, что законодатели, видя свое отставание от темпов развития интернет - преступности, стремятся законодательно регламентировать тотальный контроль государства в сети интернет, что поможет значительно облегчить процесс борьбы с интернет-преступностью.

Интернет-преступность каждого нового этапа отличается от предыдущего количественным и качественным показателями, изощренностью и общественной опасностью. Особенности ее развития, прежде всего, связаны с некоторой запоздалостью (примерно на 15–20 лет) появления интернета в России и с высоким техническим уровнем отечественных интернет-преступников, что позволило российской интернет-преступности быстро догнать, и даже в некоторых моментах обогнать, зарубежную. Прогнозировать развитие интернет-преступности в качественном и количественном аспектах достаточно сложно.

Складывается впечатление, что сегодня изобретено все, что можно изобрести. Однако преступность не стоит на месте, появляются все новые и новые виды преступлений, совершаемых посредством интернета. Мнение Р. И. Дремлюги, который считает, что интернет-преступность будет преобладать над другими видами и будет обширно влиять не только на экономические, но и на политические процессы, является актуальным и верным. Хотелось бы отметить, что никакие аппаратные, программные и любые другие средства не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности компьютерных систем и их сетей и организации взаимодействия между субъектами выявления, раскрытия и расследования интернет-преступлений в международном масштабе.

Необходимо рассмотреть также совершение киберпреступлений путем использования психологического влияния на человека стоит отметить, что это один из самых сложных по структуре расследования киберпреступление. Указанное утверждение рождается исходя из статистики касаемой расследования киберпреступлений, таким образом количество киберпреступлений в 2024 г. возросло на

24, 4 %, а мошенничество в данной сфере киберпреступлений занимает лидирующее место. Чаще всего такие преступления совершаются путем создания фальшивых ссылок на официальные сайты, создание сайтов двойников, а также звонков по видео или голосовой связи под видом сотрудников банков, ФСБ России и полиции. Проблематика предотвращения таких преступлений заключается в том, что несмотря на многочисленные оповещения граждан о наличии мошенников в обществе, люди доверяют злоумышленникам, так как они используют различные способы воздействия и манипулирования, такие как: угрозы, давление, принятие роли спасателя. Так же при расследовании данного вида преступлений, сотрудники сталкиваются с рядом сложностей, таких как: быстрое уничтожение вещественных доказательств злоумышленниками, обрывание связей с жертвой, перевод электронных денежных средств в наличные. Из-за возникающих трудностей расследование кибермошенничества с использованием методов социальной инженерии становится приближенным к невозможному.

Для решения проблем расследования следует рассмотреть различные новые технологии, включая искусственный интеллект. Для перевода денежных средств жертвы чаще всего используют мобильные телефоны, на которых существуют онлайн банки. Возможно установить функцию, которая будет высылать уведомления на экран пользователей при переводе денежных средств, содержащие в себе памятку о мошеннических действиях, способах распознавания злоумышленников и дополнительную кнопку, подтверждающую перевод. Такая функция позволит задуматься о необходимости перевода средств, а также предотвратит неразумные переводы. Так же возможно рассмотреть создание новых программ, блокирующих подозрительные ссылки, анализирующих схожие ссылки и сайты, удаляя неофициальные и не сертифицированные, такая технология позволит предотвращать подделку сайтов и создание вредоносных ссылок.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// Российская газет, № 165, 29.07.2006.
2. Федоров М. Н. Преступления, совершаемые с помощью глобальной информационной сети Интернет.
3. Батулин Ю. М. Проблемы компьютерного права / Батулин Ю. М. М.: Юрид. лит., 1991.
4. Беспалова Е. В., Широков В. А. Киберпреступность: история уголовно-правового противодействия // Информационное право. М.: Юрист, 2006, № 4 (7).
5. Дворецкий М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография / М. Ю. Дворецкий.
6. Голубев В. А. Компьютерная преступность: состояние, угрозы и прогнозы // Компьютерная преступность и кибертерроризм. Сборник научных работ: вып. № 2. Запорожье: Центр исследования компьютерной преступности, 2004.

7. The Adversarial Approach in the Pretrial Phase of Prosecution / V. V. Pushkarev, E. A. Trishkina, E. V. Tokareva [et al.] // Cuestiones Políticas. – 2020. – Vol. 37, No. 65. – P. 281–287.

8. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWQVQF.

9. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.

10. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

11. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

12. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

13. Пушкарёв, В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

14. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

Колесникова Е. А.¹,
*курсант института
подготовки сотрудников для органов
предварительного расследования
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:
Поликарпова Е. В.,
*старший преподаватель кафедры
противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя*

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ АНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СЕТИ ИНТЕРНЕТ

В условиях стремительной цифровизации современного общества особую актуальность приобретает проблема противодействия преступлениям, совершаемым с использованием систем анонимизации пользователей в сети Интернет. Анализ правоприменительной практики свидетельствует о значительном росте подобных преступлений, что обусловлено развитием технологий и появлением новых способов маскировки личности злоумышленников.

Современные системы анонимизации представляют собой сложный комплекс программных и технических решений, позволяющих пользователям скрывать свою личность и местоположение в сети Интернет. К наиболее распространенным методам обеспечения анонимности относятся: использование VPN-сервисов, прокси-серверов, специализированных анонимных сетей (Tor, I2P), а также применение различных инструментов шифрования трафика [2, с. 5–9].

Особую сложность при квалификации подобных преступлений представляет определение субъекта преступления. В отличие от традиционных составов, где личность преступника может быть установлена относительно быстро, в случае с анонимными сервисами возникает целый комплекс проблем: от невозможности определить физическое местонахождение злоумышленника до сложности установления его реальной личности.

Анализ действующего уголовного законодательства показывает недостаточную проработанность норм, регулирующих ответственность за преступления, совершаемые с использованием систем анонимизации. Существующие составы преступлений не учитывают специфику подобных деяний, что приводит к сложностям при квалификации и последующем доказывании вины.

В частности, возникает проблема определения момента окончания преступления. При совершении традиционных преступлений момент окончания четко определен и не вызывает разночтений. Однако в случае с анонимными сервисами

¹ © Колесникова Е. А., 2025.

злоумышленник может находиться в любой точке мира, что существенно усложняет установление момента окончания преступления и, как следствие, влияет на квалификацию деяния.

Серьезную проблему представляет собой оценка умысла преступника. Использование систем анонимизации само по себе может свидетельствовать о наличии прямого умысла на совершение противоправного деяния, однако доказать это в рамках уголовного процесса крайне сложно. Более того, злоумышленники часто используют многоуровневые схемы анонимизации, что делает практически невозможным установление истинных намерений лица.

Особого внимания заслуживает вопрос о необходимости введения специального состава преступления, предусматривающего ответственность за создание, модификацию, администрирование и распространение систем анонимизации [3, с.46-49]. В настоящее время подобные действия могут быть квалифицированы лишь по общим составам преступлений, что существенно снижает эффективность противодействия данной категории преступлений.

При квалификации преступлений, совершаемых с использованием систем анонимизации, возникает проблема оценки общественной опасности деяния. Использование анонимных сервисов существенно повышает потенциальный вред от преступления, поскольку позволяет злоумышленнику действовать безнаказанно длительное время и вовлекать в преступную деятельность большее количество лиц.

В правоприменительной практике часто возникают сложности при определении территориальной подсудности дела. Учитывая трансграничный характер преступлений, совершаемых с использованием систем анонимизации, возникает необходимость разработки специальных правил определения подсудности, учитывающих особенности данной категории дел.

Особую проблему представляет собой доказывание факта использования систем анонимизации. В ходе расследования необходимо установить не только сам факт использования подобных систем, но и определить конкретные методы анонимизации, примененные злоумышленником. Это требует специальных знаний и навыков от следователей, а также наличия соответствующего технического обеспечения.

В современных условиях особую актуальность приобретает вопрос о необходимости совершенствования международного сотрудничества в сфере противодействия преступлениям, совершаемым с использованием систем анонимизации. Учитывая трансграничный характер подобных преступлений, требуется разработка единых подходов к их квалификации и расследованию на международном уровне.

Анализ правоприменительной практики показывает необходимость создания специализированных подразделений в правоохранительных органах, обладающих необходимыми компетенциями для расследования преступлений, совершаемых с использованием систем анонимизации. Это позволит повысить эффективность противодействия данной категории преступлений и обеспечить надлежащую квалификацию деяний.

В качестве перспективных направлений совершенствования уголовно-правовой оценки подобных преступлений можно выделить: разработку специальных технических средств для выявления и документирования фактов использования систем анонимизации; создание единой базы данных о методах анонимизации и способах их обнаружения; разработку методических рекомендаций по квалификации преступлений, совершаемых с использованием систем анонимизации.

В заключение следует отметить, что эффективное противодействие преступлениям, совершаемым с использованием систем анонимизации, возможно только при комплексном подходе, включающем совершенствование уголовного законодательства, развитие технической базы правоохранительных органов и повышение квалификации специалистов в данной области [6, с.124-129]. Только такой подход, на наш взгляд, позволит обеспечить адекватную уголовно-правовую оценку подобных преступлений и повысить эффективность противодействия им.

В современных условиях особую актуальность приобретает проблема разработки специальных методов расследования преступлений, совершаемых с использованием систем анонимизации. Это обусловлено постоянным совершенствованием технологий анонимизации и появлением новых способов маскировки личности злоумышленников.

В частности, требуется разработка специальных методик сбора и анализа цифровых следов, оставленных злоумышленником при использовании систем анонимизации. Это позволит повысить эффективность расследования и обеспечить надлежащую квалификацию преступлений.

Особую значимость приобретает вопрос о необходимости создания специализированных образовательных программ для подготовки специалистов в области расследования преступлений, совершаемых с использованием систем анонимизации. Это позволит обеспечить правоохранительные органы квалифицированными кадрами, обладающими необходимыми компетенциями для противодействия данной категории преступлений.

Список литературы

1. Воробьев В. И. Методы защиты метаданных в формате XML // Онтология проектирования. 2018. № 2. С. 253–264.
2. Сачков И. К. Автоматизация противодействия бот-атакам // T-Comm - Телекоммуникации и Транспорт. 2014. № 1. С. 5–9.
3. Нестерович С. А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и образования. 2018. № 8. С. 46–49.
4. Шахкелдов Ф. Г., Колиев В. В. Методика раскрытия преступлений, совершаемых с использованием информационно-коммуникационных технологий // Право и практика. 2021. № 1. С. 92–95.
5. Костенко Н. С., Семененко Г. М., Пшеничкин А. А. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием

информационно-телекоммуникационных технологий, на современном этапе // Вестник Воронежского института МВД России. 2020. № 4. С. 192–196.

6. Агапов П. В. Проблемы квалификации преступлений с использованием систем анонимности в сети Интернет / П. В. Агапов // Вестник экономической безопасности. – 2023. – № 3. – С. 124–129.

7. Иванов Д. В. Правовые проблемы использования систем анонимности в сети Интернет / Д. В. Иванов // Цифровая криминалистика. – 2023. – № 1. – С. 78–85.

8. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

9. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

10. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

11. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

12. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.

13. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.

14. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Комлева М. А.¹,

курсант института подготовки

сотрудников для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Токолов А. В.,

доцент кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

МЕРЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ДИПФЕЙКА

На сегодняшний день термин «дипфейк» официально не закреплён в технических стандартах и нормативных актах. Его, скорее, можно считать общеупотребительным выражением, хотя оно широко используется в средствах массовой информации и кинематографической индустрии. Под данным термином понимается контрафактный материал, созданный путем использования методов искусственного интеллекта, включая трансформацию внешности и голосовых характеристик знаменитостей для интеграции их в различные медиафайлы. Основной целью данной манипуляции является создание убедительной иллюзии участия определенного лица в событиях или действиях, выгодных третьим лицам. Сам термин «дипфейк» возник в конце 2017 г. благодаря псевдониму пользователя онлайн-ресурса Reddit – Deepfakes, который начал совмещать лица популярных актрис с изображениями порно-актеров и публиковал получившиеся ролики. Позже другой участник форума Reddit, известный как Deepfakeapp, разработал программу FakeApp, доступную широкому кругу пользователей, позволяющую самостоятельно создавать подобные материалы без глубоких познаний в сфере информационных технологий. Сегодня существует целый ряд аналогичных приложений, совместимых с различными операционными системами (Windows, macOS, Linux, Android, iOS). Для большинства пользователей технология дипфейков служит исключительно средством развлечения, однако она приобрела особую привлекательность среди преступников, использующих ее для противоправных целей. Современные разработки в области искусственного интеллекта значительно повысили уровень достоверности подобного вида контента. Важно понимать различие между сложными объектами информационной среды, такими как дипфейки, и дешевыми подделками («cheapfakes»), мелкими фальшивками («shallowfakes») и прочими видами недостоверной информации, создаваемыми без применения передовых технологий. Подобные программы позволяют любому человеку независимо от уровня квалификации легко овладеть процессом производства дипфейков. Существует несколько классификаций дипфейков: по

¹ © Комлева М. А., 2025.

способам реализации, категориям авторов, целям использования, типам злодеяний и уровню нанесенного вреда. Методы создания включают замену лица, контроль над мимикой и жестами, симуляцию движений губ, воспроизведение речи, синтез визуальных образов, текстовую генерацию, передачу стилистических особенностей, ретуширование и трехмерное моделирование. Например, программа Snapchat начиная с 2014 г. предлагает своим пользователям менять внешний вид с использованием фильтров, идентифицирующих лицо, позволяя буквально увидеть себя постаревшим. Можно выделить пять типов разработчиков дипфейков: энтузиасты и любители; политики и государства, включая зарубежные правительственные структуры и активистов; киберпреступники и мошенники; компании коммерческого сектора; представители СМИ. Среди возможных мотиваций для совершения преступлений посредством дипфейков выделяются нарушения личных свобод, компрометация репутации, сексуальное преследование, производство порнографической продукции, хищение денежных средств, ущемление интеллектуальных прав, вмешательство в личную жизнь, фабрикация доказательств, манипуляции уголовными делами, провоцирование общественных беспорядков и политическая дестабилизация общества. Дипфейки сами по себе являются технологически нейтральными инструментами, однако потенциально представляют серьезную угрозу как для отдельных граждан, так и для компаний и целых государств. Их применение способно спровоцировать политическую нестабильность, социальные конфликты, утрату доверия, тревожность, агрессию и даже физические столкновения. Таким образом, данные явления оказывают значительное влияние на общественные процессы и требуют повышенного внимания со стороны органов власти и экспертов в области информационной безопасности.

Правовая основа многих стран не готова должным образом справляться с технологическими вызовами, связанными с развитием технологий дипфейков. В числе значимых исследований стоит выделить следующие работы: статья «Этика дипфейков» от аналитического центра Observer Research Foundation, работа «Дипфейки: злой умысел или развлечение» бизнес-школы им. Келли Университета Индианы и юридический обзор в научном журнале «Illinois Law Review» под названием «AI Deepfakes. Утка жареная?», а также множество других исследований, направленных на снижение негативных последствий от использования технологий дипфейков. Создание и улучшение технологий защиты от дипфейков стало одним из ключевых направлений глобальной кибербезопасности. В конце 2021 г. Россия включила это направление в дорожную карту «Новые коммуникационные интернет-технологии», разработанную «Ростелекомом» и утвержденную Правительственной комиссией по цифровому развитию. Эксперты прогнозируют, что к 2024 г. объем мирового рынка технологий распознавания дипфейков вырастет с 10,9 млн руб. до 119 млн рублей. Постепенно разрабатываются инструменты для идентификации фальсифицированных изображений, но они только на начальной стадии, поскольку дипфейк – это явление, созданное искусственным интеллектом, и для его выявления нужны аналогичные технологии. К концу 2022 г. МВД России планирует получить программу «Зеркало» для распознавания видео с заменой лиц. При разработке дипфейка с использованием

самых современных технологий всегда будет существовать определенная задержка между появлением новых технологий распознавания и возможностью их применения для выявления дипфейков. Вопрос правового регулирования дипфейков становится все более актуальным. Их возможности использования весьма разнообразны, что делает полный запрет на создание и распространение таких материалов невозможным. На данный момент в мире существуют два примера ограничения такого контента. В Калифорнии, США, ряд IT-компаний запретили дипфейки, касающиеся кандидатов на выборах. В Китае с 2020 г. существует уголовная ответственность за поддельные видео и другие случаи распространения ложной информации. Тем, кто применяет технологию в развлекательных или законных целях, рекомендуется маркировать видео, указывая, что это не подлинная запись. Упоминается, что использование технологий дипфейка может угрожать национальной безопасности, подрывать социальную стабильность, нарушать общественный порядок и ущемлять законные права и интересы граждан. Одним из решений проблемы дипфейков является необходимость постоянного повышения квалификации сотрудников правоохранительных органов. Изучение основ информационной безопасности и совершенствование навыков борьбы с кибермошенниками позволит им быть в курсе текущих событий в интернет-сообществе и эффективно решать возникающие проблемы.

Список литературы

1. Грачева Ю. В. Цифровые технологии и безопасность личности / Ю. В. Грачева // Криминалист. – 2019. – №. 1. – С. 24–27.
2. Проект «Верблюды» поможет МВД России распознать дипфейки [Электронный ресурс]. URL: <https://www.securitylab.ru/news/519728.php>.
3. Tim Hwang / «Deepfakes: A Grounded Threat Assessment» // Center for Security and Emerging Technology.
4. Криминальная жизнь дипфейков [Электронный ресурс]. URL: https://zavtra.ru/blogs/kriminal_naya_zhizn_dipfejkov.
5. «Аферы с дипфейками: какие угрозы скрываются за искусственными лицами?» [Электронный ресурс]. URL: <https://www.securitylab.ru/blog/company/PandaSecurityRus/351217.php>.
6. Gracheva Yu.V. Digital technologies and personal security / Yu.V. Gracheva // Criminalist. – 2019. – №. 1. – Pp. 24–27.
7. The Camel project will help the Ministry of Internal Affairs of Russia to recognize deepfakes [Electronic resource]. URL: <https://www.securitylab.ru/news/519728.php>.
8. Tim Hwang / «Deepfakes: A Grounded Threat Assessment» // Center for Security and Emerging Technology.
9. The criminal life of deepfakes [Electronic resource]. URL: https://zavtra.ru/blogs/kriminal_naya_zhizn_dipfejkov.
10. "Deepfake scams: what threats are hidden behind artificial faces?" [Electronic resource]. URL: <https://www.securitylab.ru/blog/company/PandaSecurityRus/351217.Php>.

11. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
12. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарев // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWOVQF.
13. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.
14. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
15. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
16. Пушкарев, В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
17. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

Кондаков Н. Д.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Рудин А. В.,

*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

DEEPFAKE-ТЕХНОЛОГИИ: УГРОЗЫ И МЕТОДЫ ОБНАРУЖЕНИЯ

В настоящее время множество людей проводят достаточно много времени в сети Интернет, на ее просторах можно встретить огромное множество информации, что-то будет являться правдой, что-то ложью, но основная проблема заключается в том, что не все могут различать достоверную информацию от ложной. С момента появления искусственного интеллекта в массовом пользовании стали появляться и плоды его работ, одним из таких является Deepfake фото/видео/аудио контент. Технология Deepfake – это синтетически созданные изображения, видеоролики или аудиокomпозиции, которые с высокой реалистичностью подделывают реальные записи. Сам термин «Deepfake» объединяет в себе следующие понятия «deep learning» что в переводе обозначает «глубинное обучение» и «fake» «обман, подделка». Углубляясь в историю подобного контента, можно заметить, что подобный контент был и до введения искусственного интеллекта в массы, но тогда для создания подобного требовалось приложить массу усилий и времени, сейчас же для получения результата стоит лишь обратиться к чат-боту или приложению, написать запрос и в течение нескольких минут получить желаемый результат. Сама технология работает при помощи открытых алгоритмов машинного обучения и библиотек, что позволяет достичь высокого качества контента, при помощи них нейросеть обучается, запоминает мимику, движения, тональность и после сопоставляет исходный материал с тем, что должно получиться, и как итог данной операции появляется контент, который выглядит как реалистичный, хотя таковым не является.

Первые поддельные видеоролики появились в 2017 г., выглядели они достаточно забавно, в основном это были любительские видеофайлы содержащие лица знаменитостей. Они не представляли из себя серьезной угрозы, так как выглядели так что практически сразу же было понятно, что представленная видеокomпозиция является не настоящей. Однако спустя немного времени, технология стала представлять серьезную угрозу, так, например в 2018 г. было опубликовано

¹ © Кондаков Н. Д., 2025.

фальшивое видео с экс-президентом США Бараком Обамой, где он якобы оскорбляет Дональда Трампа.

В 2019 г. в сети появился ролик со спикером палаты представителей конгресса США Ненси Пелоси, в нем автор при помощи искусственного интеллекта изменил речь спикера так, что она плохо выговаривала слова, пользователи, увидевшие данный видеоролик решили, что политик находится в состоянии алкогольного опьянения. Данный инцидент перерос в большой скандал, и лишь спустя некоторое время было доказано, что речь Пелоси была сгенерирована при помощи нейросетей.

Кроме политических информационных войн технология Deepfake создает риски в области информационной безопасности. Таким примером является целевой фишинг, он направлен на обман конкретных сотрудников определенных компаний на совершение действий или операций, благодаря которым мошенники могут внедриться в систему управления компании и нанести значительный ущерб (оплатить платежное поручение, отправить документы, сбросить учетные данные пользователей, удалить базы данных).

Происходит это следующим образом, сотрудник компании получает голосовое сообщение или видеозвонок от генерального директора компании, в котором его просят оплатить приложенные к сообщению счета, либо же выполнить действия на рабочем компьютере, которые позволят мошенникам получить доступ к системе в обход системы безопасности, при этом к обращению к сотруднику будет по имени, возможно в нем будут упомянуты какие-либо факты которые напрямую связаны с его обязанностями или события недавно произошедшие в компании, из-за чего сотрудник даже не задумается о том, что сообщение может быть поддельным.

Так, в 2021 г. стало известно, что преступники завладели суммой в 35 миллионов долларов США из банка в ОАЭ. Мошенник связался с менеджером и представился генеральным директором компании, с которым у них ранее были сделки, подкрепляя это электронными письмами от банка и юриста сопровождающего сделки в прошлом, все выглядело настоящим, убедило менеджера в том, что говорит он с генеральным директором, а компания действительно находится в процессе крупной коммерческой сделки на сумму 35 миллионов долларов США. Впоследствии он последовал указаниям мошенника и совершил несколько денежных переводов от компании на предоставленный счет. Из материалов суда следует, что голоса были идентичными, а следователи полиции Дубая сделали выводы о том, что данное преступление было совершено при помощи технологии «подмены голоса».

Однако не только зарубежный опыт позволяет понять опасность данной технологии. В Российской Федерации так же зарегистрированы попытки мошенничества с использованием технологии «Deepfake». Так, в начале 2023 г. в сети Интернет появился видеоролик, в котором женщина отвечает на телефонный звонок. Она слышит голос сына, который отправляет ей номер телефона и просит перевести ему 1000 рублей на подарок другу, при этом происходит это в момент, когда мама и сын находятся рядом. За подобные деяния Уголовным кодексом РФ

предусмотрена ответственность в соответствии со статьями главы 21 «Преступления против собственности»

Также стоит отметить, что технология «Deepfake» не только помогает преступникам в обмане жертв, но и создает проблемы в их поимке, ведь с каждым днем все больше и больше граждан сталкиваются с видеозвонками в мессенджерах от якобы представителей банков, отвечая на подобный звонок, жертва видит человека в одежде с логотипами банка, на фоне так же располагается логотип, лицо, голос, и прочие черты можно запомнить, и в случае чего обратиться в полицию. Однако злоумышленники подменяют изменяют голоса и лица, из-за чего выявить реальную информацию о человеке становится невозможным.

Распознать технологию «Deepfake» в настоящее время программным методом не является возможным. Ведутся активные исследования в этой области, но фактически это противостояние двух стихий, где первая пытается обойти возможные ограничения, а вторая – создать барьеры, благодаря которым обход будет являться невозможным.

Крупные компании, такие как Microsoft, Intel, Ассоциация компаний Google, занимаются разработкой синтетических меток. Идея заключается в том, чтобы отметить специальным «водяным знаком» весь сгенерированный контент. Внешне такая метка никак не выделяется и не видна при использовании, но используя определенный алгоритм, будет понятно, сгенерирован ли представленный контент, либо же является настоящим.

Сама идея достаточно отлично должна себя показать, однако у нее есть ряд ограничений, которые позволяют с легкостью ее обходить. В частности, любое изменение сгенерированного файла, будь то изменение размера, длительности, формата, позволят устранить эти отметки. Поэтому нужна технология, при которой удаление «водяных знаков» будет являться невозможной.

Однако все-таки есть способы распознать технологию «Deepfake».

Первым способом будет являться самый простой способ – это включить критическое мышление. Если на видео человек говорит вещи, которые ему не свойственны или вызывают подозрение, можно попробовать найти данное видео на просторах сети Интернет. Сделать это можно по ключевым фразам или событиям. Так же в некоторых браузерах существует функция поиска по фото, используя снимок содержащий элемент видеоролика, можно попробовать найти оригинальный источник данного видеофайла.

Второй способ – это внимательность. Если с вами связался человек при помощи видеосвязи или в общении использует голосовые сообщения, внимательно проследите за его речью, мимикой, движениями, изменениями тембра голоса. Несмотря на постоянное развитие искусственного интеллекта, его использование все-равно может быть заметно при внимательном рассмотрении. Изменение формы бровей, расхождение движения губ от произносимых слов, разное произношение одних и тех же слов – все это может являться признаками использования технологии «Deepfake».

Третий способ связан со вторым, но направлен он на суть работы технологии. Обычно накладывается именно лицо, поэтому стоит обратить внимание на лобную часть лица, а именно на ту часть, где начитаются волосы. Если оттенок кожи

отличается или данный участок сильно расплывается, то с высокой вероятностью, вы столкнулись с технологией «Deepfake». Так же отсутствие или несоответствие эмоций, может являться признаком использования искусственного интеллекта.

В заключении важно сказать, что в сфере информационно-телекоммуникационных технологий наблюдается непрерывный прогресс, и нейросети становятся все более совершенными. Это приводит к тому, что Deepfake-технологии становятся все более доступными, однако с развитием этих возможностей возникают серьезные угрозы для личной безопасности и социальной стабильности. Данная технология может использоваться не только для креативного самовыражения, но и как инструмент манипуляции и распространения дезинформации. Использование фальшивого контента может серьезно подорвать репутацию людей, привести к правовым спорам и даже оказать влияние на политические события. Поэтому в условиях современной цифровой среды осторожность при работе в сети Интернет, особенно при обращении с личными данными, становится жизненно важной.

Также стоит отметить, что необходимость разработки действенных методов выявления фальсификаций становится все более актуальной. На сегодняшний день уже применяются алгоритмы машинного обучения, которые помогают обнаруживать характерные признаки искусственного создания контента. Улучшение методов обнаружения – это ключевой шаг в борьбе с угрозами, которые могут исходить от Deepfake-технологии. Важно, чтобы исследователи и специалисты в области информационной безопасности продолжали сотрудничать, делиться знаниями и разрабатывать новые решения для снижения рисков.

Таким образом, в условиях стремительно меняющегося цифрового мира важно оставаться информированным и внимательным, чтобы обеспечить безопасность и защиту своих личных данных. Только комплексный подход поможет справиться с угрозами, которые возникают совместно с развитием Deepfake-технологий.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025).
2. Мошенники украли \$35 млн у банка ОАЭ с помощью дипфейка голоса его главы [Электронный ресурс] URL: <https://www.tadviser.ru/index.php> /Статья: Мошенничество_с_дипфейками.
3. Осторожно, deepfake. Как распознать мошенника на видео [Электронный ресурс] URL: <https://www.sberbank.ru/ru/person/kibrary/articles/ostorozhno-dipfejk-kak-uznat-moshennika-na-video>.
4. Что такое дипфейки, для чего их используют и чем они опасны [Электронный ресурс] URL: <https://practicum.yandex.ru/blog/hto-takoe-deepfake-i-kak-zashchititsya/>.

5. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
6. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
7. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
8. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
9. Константинов А. В. Перспективы развития и использования искусственного интеллекта в целях противодействия преступлениям в сфере информационно-телекоммуникационных технологий / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов, Москва, 30 марта 2023 года / Сост. А.В. Константинов. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 80–82.
10. Соломатина А. Г. К вопросу о понятии компьютерной информации и преступлениях, совершаемых в ее сфере / А. Г. Соломатина, В. В. Пушкарёв // Вестник экономической безопасности. – 2024. – № 5. – С. 149–155. – DOI 10.24412/2414-3995-2024-5-149-155. – EDN KWQVQF.
11. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
12. The Adversarial Approach in the Pretrial Phase of Prosecution / V. V. Pushkarev, E. A. Trishkina, E. V. Tokareva [et al.] // Cuestiones Políticas. – 2020. – Vol. 37, No. 65. – P. 281–287.

Коротеев Д. А.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Михайленко Н. В.,

*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ: ПРЕИМУЩЕСТВА И УЯЗВИМОСТИ

Биометрическая аутентификация – это процесс обеспечения безопасности, который основан на технологии распознавания личности человека по его биологическим характеристикам. Благодаря уникальности данных характеристик удастся подтвердить, является ли человек именно тем лицом, за которое он себя выдает. Биометрические данные каждого человека, прошедшего процедуру биометрической аутентификации, загружаются в базу данных и являются уникальными. После чего при запросе доступа к информационному ресурсу системы биометрической аутентификации берут введенные данные пользователя и сравнивают их с теми данными, которые хранятся в системе. Если удастся провести аутентификацию, то она определяется как успешная, после чего аутентифицированный пользователь получает доступ к какому-либо ресурсу.

Биометрическая аутентификация может быть использована в различных отраслях, например, для доступа на какие-либо объекты, как пример, я могу привести здания и отдельные помещения, так и, например при допуске к разнообразным информационным ресурсам, такие как телефон, различные приложения на нем и другие информационные системы.

Естественно, что биометрическая аутентификация повышает безопасность, так как сложно подделать различные индивидуальные биологические параметры человека, но помимо этого она также очень удобна, поскольку невозможно забыть или потерять свои биометрические данные, более того они всегда будут при вас, что позволит получать доступ к различным ресурсам в любое время и при любых обстоятельствах.

Как работает биометрическая аутентификация?

Аутентификация с использованием биометрических данных стала очень распространенной в наше время, каждый человек вместо того, чтобы вводить пароль на своем телефоне пользуется отпечатком пальца, либо разблокирует телефон с помощью лица, помимо безопасности это очень удобно, потому что люди могут

¹ © Коротеев Д. А., 2025.

отказаться от паролей, которые им приходилось бы запоминать и где-то хранить).

Биометрическая технология состоит из следующих компонентов

- 1) считывающее устройство для записи биометрических характеристик;
- 2) программное обеспечение для преобразования считанных биометрических характеристик в цифровой формат и сравнения с заданными значениями;
- 3) база данных для безопасного хранения эталонных биометрических данных и истории процессов аутентификации.

Преимущества и недостатки биометрической аутентификации:

Благодаря предыдущим абзацам мы выяснили что представляет из себя биометрическая аутентификация, что позволит мне определить в чем заключается ее преимущество перед другими способами аутентификации.

К преимуществам мне хотелось бы отнести:

- 1) данные, используемые для биометрической аутентификации, невозможно украсть так как это все человек всегда носит с собой, а также эти данные очень трудно подделать;
- 2) удобство и простота в использовании, не нужно запоминать и куда-либо записывать, экономия времени, поскольку приложить палец к телефону гораздо проще и быстрее, чем вводить пароль;
- 3) не нужно передавать другим пользователям, это можно отнести как к преимуществам, так и к недостаткам;

К недостаткам можно отнести:

- 1) требует больших вложений, так как создать биометрическую систему, например, в каком-то предприятии достаточно затратно, как по времени, так и по денежным средствам;
- 2) могут возникнуть сбои при аутентификации пользователя, если система загрузит и не ей не удастся считать данные пользователя корректно;
- 3) база данных, где хранятся биометрические данные пользователей может быть взломана, что создаст определенные способы для подделки биометрических данных со стороны преступников;
- 4) необходимость наличия определенных окружающих условий, например, некоторые устройства не могут аутентифицировать лицо человека, который находится в темноте, поэтому в таких условиях пользователю приходится либо включать светя, либо если данная ситуация произошла на улице найти источник света;

5) наличие ошибок первого и второго рода. Ошибки первого рода – те ошибки, которые заключаются в том, что система не пропускает легального пользователя в систему, а ошибки второго рода, когда наоборот система пропускает человека, который не является легальным пользователем;

6) и заключительная, самая главная проблема биометрической аутентификации как по мне является то, что, если пользователь утрачивает что-то из биометрических характеристик, например, в результате травмы (облили лицо кислотой, порезал палец), его аутентификация по этим признакам становится невозможной.

В заключении мне хотелось бы отметить, что биометрическая аутентификация совсем недавно вошла в наш быт, но при этом она с каждым днем эволюционирует и становится более удобной, надежной и быстрой. В скором будущем, я считаю, она станет еще более качественной и не будут допускаться ошибки, которые я указывал, станет меньше минусов и больше плюсов, по моему мнению, скоро почти все пользователи перейдут на биометрическую аутентификацию поскольку это очень удобно и надежно.

Список литературы

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в ред. от 27 июля 2006 года).
2. Иванов М. С. Анализ уязвимостей и актуальных биометрических методов аутентификации в системах безопасности / М. С. Иванов. – Текст: непосредственный // Молодой ученый. – 2023. – № 20 (467). – С. 4–7.
3. Кураков В. И., Худадян А. С., Баева У. М. Научная статья на тему «Анализ уязвимостей биометрических методов аутентификации».
4. Единая биометрическая система: доступ к новым сервисам безопасной цифровой России [Электронный ресурс]. Режим доступа: bio.rt.ru/documents/marketing/?SECTION_ID=191.
5. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
6. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
7. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
8. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
9. Константинов А. В. Перспективы развития и использования искусственного интеллекта в целях противодействия преступлениям в сфере информационно-телекоммуникационных технологий / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов, Москва, 30 марта 2023 года / сост. А. В. Константинов. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 80–82.
10. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токотов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

11. The Adversarial Approach in the Pretrial Phase of Prosecution / V. V. Pushkarev, E. A. Trishkina, E. V. Tokareva [et al.] // Cuestiones Políticas. – 2020. – Vol. 37, No. 65. – P. 281–287.

12. Михайленко Н. В. Отдельные проблемы цифровизации органов внутренних дел Российской Федерации / Н. В. Михайленко // Актуальные проблемы кибербезопасности в сети Интернет : Сборник научных трудов Всероссийской конференции, Москва, 23 апреля 2020 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2020. – С. 102–105.

Крестинина А. В.¹,

курсант института подготовки

сотрудников для органов

предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Константинов А. В.,

заместитель начальника кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

РАЗВИТИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РОССИИ

Искусственный интеллект (далее – ИИ) стал ключевым элементом современной технологической революции, оказывая значительное влияние на экономику, безопасность и социальную сферу. Россия, обладая богатым научным потенциалом, активно развивает ИИ, стремясь занять лидирующие позиции в этой области. Наверное, каждый человек в 2024 г. слышал про такое понятие как искусственный интеллект, но мало кто задавался вопросами: как он появился и какие пределы его развития? Развитие ИИ в России имеет глубокие корни, начиная с советского периода, когда были заложены основы кибернетики и математической логики. Советские ученые внесли значительный вклад в теорию автоматического управления и моделирования. Еще в 1950-х гг. известный английский математик Алан Тьюринг выдвинул идею; может ли машина обладать человеческим разумом? После этого в философском журнале была опубликована работа Тьюринга «Вычислительные машины и разум», где был затронут тест на интеллект у машины. Суть теста довольно проста; проверяющий взаимодействует с одним компьютером и одним человеком. На основании ответов на вопросы он должен определить, с кем он разговаривает: с человеком или компьютерной программой. Задача компьютерной программы – ввести человека в заблуждение, заставив сделать неверный выбор» Это считается точкой отсчета развития технологий с использованием машинного интеллекта. Однако в 1990-е гг. развитие ИИ замедлилось из-за экономических и политических преобразований. С начала 2000-х гг. наблюдается возрождение интереса к ИИ, что связано с развитием цифровых технологий и глобальными тенденциями.

Вопрос о развитии искусственного интеллекта в нашей стране был поднят еще в начале 1960 г. В период с 1960 по 1980 гг. под научным руководством доктора технических наук, профессора Д. А.Поспелова были созданы ряд комплексов и направлений по развитию электронных вычислительных машин. Более подробно раскрываются идеи Поспелова в таких научных трудах как; «Логические методы анализа и синтеза схем», «Мышление и автоматы», «Введение в теорию

¹ © Крестинина А. В., 2025.

вычислительных систем» и другие не менее важные научные работы [1]. Также в этот период были созданы специальные логические модели, отображающие в памяти технической системы полный набор необходимых знаний о фундаментальных связях между явлениями окружающей среды. Эти модели получили общее название «псевдофизических логик». В СССР также стал набирать популярность чемпионат по игре в шахматы среди компьютерных программ, получившая названия Каисса. В 1968 г. вышла книга советского философа Э. В. Ильенкова «Об идолах и идеалах», в которой автор отрицал возможность создать машинный интеллект, который будет превосходить разум людей, потому что человек самое умное существо на планете.

К началу 2000-х гг. на российский рынок стали поступать импортные ЭВМ, среди которых был Sony PlayStation, компьютеры с операционной системой Windows XP и другая техника. Одним из первых русских проектов по созданию стал процессор Эльбрус 2000 (E2K), который был самым мощным компьютерным процессором на территории стран СНГ и ряд европейских стран. В сентябре 2009 г. по инициативе российского Президента Д. А. Медведева был разработан проект по созданию научно-технологического инновационного комплекса «Сколково». На 2024 г. комплекс Сколково зарекомендовал себя больше с положительной стороны, где создаются проекты как по развитию информационных технологий, так и промышленных.

На сегодняшний день нет однозначного закрепления определения «искусственный интеллект». В Указе Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» закреплено понятие сильный искусственный интеллект – тип искусственного интеллекта, который способен выполнять различные задачи, взаимодействовать с человеком и самостоятельно (без участия человека) адаптироваться к изменяющимся условиям [2]. В 2019 г. был подписан Указ Президента Российской Федерации № 490 «О развитии искусственного интеллекта в Российской Федерации», который определил цели и задачи в области ИИ. Основные направления включают поддержку научных исследований, развитие программного обеспечения, повышение доступности данных и аппаратного обеспечения, а также подготовку квалифицированных кадров.

В Указе говорится, что искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их [3]. По словам директора Центра стратегической аналитики и больших данных ИСИЭЗ НИУ ВШЭ Константина Вишневского, «После первой волны визионерского восприятия и завышенных ожиданий к технологиям ИИ решения на их основе постепенно становятся неотъемлемым инструментом бизнеса и применяются практически во всех сферах деятельности – от мониторинга сельхозугодий и управления космическими аппаратами до помощи в написании научных работ и новостей СМИ».

Российские компании активно развивают собственные решения в области ИИ. Сбербанк представил модель GigaChat, а Яндекс – YandexGPT, которые являются

аналогами зарубежных генеративных моделей. Компания «Наносемантика» специализируется на обработке естественного языка и разработке виртуальных ассистентов, используя собственную платформу PuzzleLib. В транспортной сфере компания Navio разработала полностью автономный тягач Navio L5, не имеющий места для водителя, оснащенный радаром и видеокамерами для обеспечения безопасности и эффективности перевозок. В 2024 г. Россия объявила о создании AI Alliance Network совместно с странами БРИКС и другими государствами, включая Сербию и Индонезию. Цель альянса – совместные исследования, регулирование ИИ и развитие рынков для продуктов на основе ИИ. Это сотрудничество направлено на снижение зависимости от западных технологий и продвижение собственных решений на международной арене.

Подводя итоги, мы можем сказать, что искусственный интеллект играет важное значение в развитии информационного общества России. В сфере внедрения технологий искусственного интеллекта более 30 процентов организаций, осуществляющих деятельность в различных отраслях экономики, применяют технологии для выполнения прикладных задач, в социальной сфере эти технологии используются, например, в российских медицинских организациях для заполнения медицинской документации голосом. Благодаря системе «Безопасный город» сократилось число совершаемых преступлений, а система «Паутина» помогает ГАИ МВД России отследить угнанный, преследуемый автомобиль при помощи камер видеонаблюдения. В научной сфере функционируют 6 крупнейших исследовательских центров в области развития искусственного интеллекта. Такими являются: «Национальный исследовательский университет "Высшая школа экономики"», «Московский физико-технический институт (национальный исследовательский университет)», «Национальный исследовательский университет ИТМО», автономная некоммерческая образовательная организация высшего образования «Сколковский институт науки и технологий», автономная некоммерческая организация высшего образования «Университет Иннополис», федеральное государственное бюджетное учреждение науки Институт системного программирования имени В.П. Иванникова Российской академии наук. Развитие искусственного интеллекта в России является приоритетным направлением государственной политики. Благодаря стратегическому планированию, инвестициям и развитию собственного научного потенциала, Россия стремится занять достойное место в глобальной ИИ-экосистеме. Реализация намеченных целей позволит не только повысить конкурентоспособность экономики, но и обеспечить технологический суверенитет страны.

Список литературы

1. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества Российской Федерации на 2017–2030 годы». <https://base.garant.ru/71670570/>.
2. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». <https://base.garant.ru/72838946/>.

3. Национальная стратегия развития искусственного интеллекта на период до 2030 года [Электронный ресурс] // Официальный интернет-портал правовой информации. <https://ai.gov.ru/national-strategy/>.
4. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
5. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
6. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
7. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
8. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Крутова Д. В.¹,
 командир отделения института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
 заместитель начальника кафедры противодействия преступлениям
 в сфере информационно-телекоммуникационных технологий
 Московского университета МВД России имени В.Я. Кикотя,
 кандидат юридических наук, доцент

ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ, СОВЕРШЕННЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие информационно-телекоммуникационных технологий и внедрение их в различные сферы общества, с одной стороны, позволяет сократить организационные, финансовые, временные, кадровые и прочие издержки, благотворно влияют на создание основы для аккумуляции персональных, коммерческих, государственных и иных данных, охраняемых законом. Однако, с другой стороны, всеобщее внедрение порождает развитие преступности, по данным ГИАЦ МВД России количество преступлений за 2024 г. составляет 765365, что на 13.1 % выше, чем за аналогичный период в 2023 г. [1]. Следовательно, правоохранительным органам необходимо постоянно вырабатывать методику противодействия таким преступлениям.

Целью данной статьи является изучение мер по противодействию преступлений в сфере использования информационно-телекоммуникационных технологий, вырабатываемых и применяемых правоохранительными органами.

Серьезной угрозой информационной безопасности для Российской Федерации являются общественно опасные деяния, которые совершаются с использованием информационно-телекоммуникационных технологий. Согласно Доктрине информационной безопасности России, развитие потенциала правоохранительных органов является основной мерой обеспечения национальной безопасности.

Одно из важнейших направлений деятельности правоохранительных органов, является в том, числе и обеспечение информационной безопасности. Однако согласно статистике ГИАЦ МВД России, раскрываемость данных преступлений оставляет желать лучшего, так раскрываемость данных преступлений в виде таблицы приведем ниже (рис.1):

¹ © Крутова Д. В., 2025.

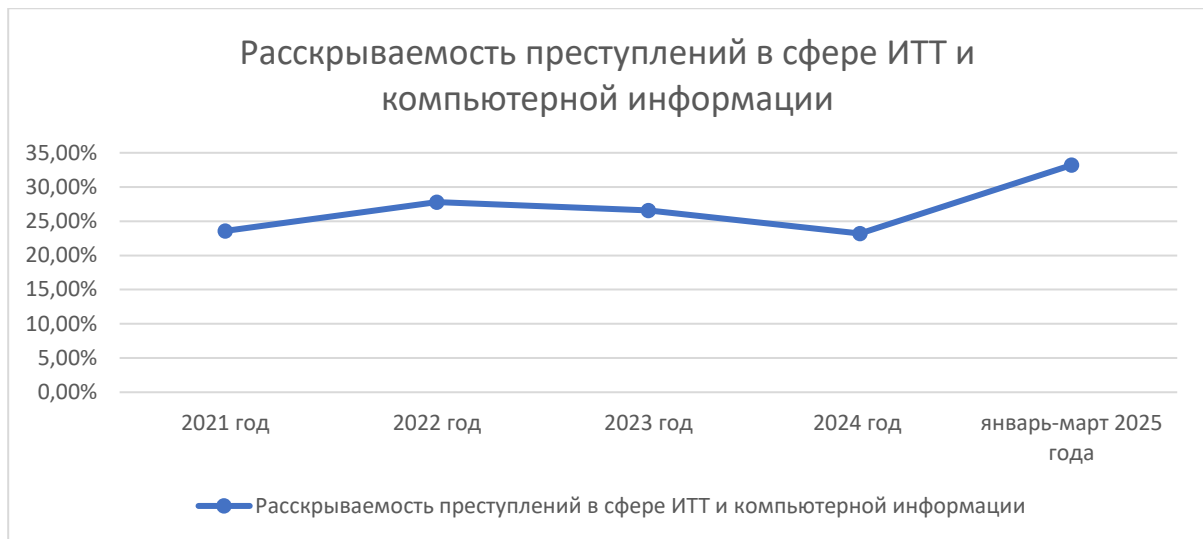


Рис.1. Раскрываемость преступлений

Одной из главных причин высокого уровня ИТ-преступности является нехватка специалистов в МВД России. Злоумышленники используют сложные методы, такие как анонимизация, подмена номеров телефонов, временные SIM-карты и виртуальные кошельки для хищения средств. Борьба с такими преступлениями требует высококвалифицированных сотрудников, разбирающихся в ИТ.

В «Доктрине информационной безопасности РФ» подчеркивается, что ИТ стали неотъемлемой частью всех сфер жизни. Это усложняет работу правоохранительных органов, так как киберпреступники часто находятся за границей, а шифрование скрывает их местоположение [2].

В 2022 г. в МВД России создали Управление по борьбе с противоправным использованием информационных технологий (УБК МВД России). Оно специализируется на противодействии преступлениям в цифровой сфере.

Кроме МВД России, борьбой с преступлениями в интернете занимается Следственный комитет РФ. В его структуре есть отдел по расследованию особо тяжких международных преступлений, включая киберхищения и вымогательство.

ФСБ России через Центр информационной безопасности также защищает от преступлений в интернете, включая терроризм и экстремизм. Центр занимается технической защитой сетей и оперативной работой в интернете.

А. А. Кашкаров подчеркивает, что предупреждение преступлений экстремистской направленности в интернете требует комплексного подхода. Блокировка сайтов не должна быть единственным методом [3].

Для эффективной работы правоохранительных органов необходимо взаимодействие с другими административными структурами, такими как ГосСОПКА, НКЦКИ и ФинЦЕРТ. Эти организации выполняют контрольно-надзорные и другие функции в сфере телекоммуникаций.

ГосСОПКА – это система для обнаружения, предупреждения и ликвидации кибератак на критическую информационную инфраструктуру России. Она включает сертифицированные отечественные средства и технологии для автоматизированного реагирования на инциденты. ГосСОПКА также обеспечивает обмен

информацией и криптографическую защиту каналов связи. Координацию деятельности в рамках системы осуществляет Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

ФинЦЕРТ – аналогичная система для финансового сектора, которая занимается сбором и передачей данных о киберинцидентах между участниками финансового рынка, правоохранительными органами, операторами связи и другими организациями в сфере информационной безопасности.

По запросам правоохранительных органов Роскомнадзор предоставляет данные о провайдере и местоположении злоумышленника, если преступление совершено через интернет-портал или личный сайт. Также Роскомнадзор может блокировать сайты, содержащие незаконный контент.

В России действуют государственные сервисы и системы на основе искусственного интеллекта для борьбы с противоправным контентом:

«Чистый интернет» – автоматизирует поиск запрещенного контента, провокаций и пропаганды.

«Бот-ферма» – создает фейковые аккаунты и имитирует активность в соцсетях для сбора информации из закрытых групп и пресечения экстремистских и террористических угроз.

«Вепрь» – ищет материалы о терроризме, экстремизме, критике властей, пропаганде ЛГБТ, наркомании, уклонении от армии, суицидальных призывах и других нарушениях.

«Окулус» – анализирует фото, видео и текст на предмет запрещенной информации с помощью нейросетей.

«Кабинет оперативного взаимодействия» – обеспечивает защищенное общение сотрудников Роскомнадзора с силовыми ведомствами для обмена информацией о выявленных угрозах и координации действий.

Преступления, совершаемые с использованием информационно-телекоммуникационных технологий, представляют серьезную экономическую угрозу. Они не знают географических границ, что усложняет их выявление и расследование. Такие преступления могут быть совершены как в России, так и за ее пределами, что затрудняет работу правоохранительных органов.

В связи с этим необходимо привлекать к расследованию узкопрофильных специалистов, включая IT-экспертов и технических специалистов. Это обусловлено ростом числа таких преступлений: в 2023 г. их количество увеличилось на 29,7 % по сравнению с 2022 г.

В сфере IT-технологий существует множество форм преступлений: корыстные, идеологические, направленные на дестабилизацию государства или общества, а также связанные с нарушением работы телекоммуникационных сетей, угрожающие жизни и здоровью людей, и другие. По статистике, каждый второй россиянин сталкивался с мошенничеством в интернете, более половины – с утечкой персональных данных, а 82 % [4] – с попытками преступлений в телекоммуникационных сетях. Увеличивается количество случаев несанкционированного вмешательства в критическую информационную инфраструктуру России, что подчеркивает масштаб проблемы.

Преступления в сфере информационно-коммуникационных технологий трудно раскрыть из-за недостатка специализированной техники [5], технологий и квалифицированных кадров в органах внутренних дел (ОВД). Особенно сложно расследовать киберпреступления транснационального характера, когда злоумышленник находится за пределами России, или когда средства шифрования скрывают его местоположение.

Еще одной причиной низкой раскрываемости таких преступлений является небольшой размер хищений (чаще всего от 10 до 30 тыс. рублей), который несоизмерим с затратами на их расследование. Это отпугивает не только правоохранителей, но и самих потерпевших, которые не видят смысла в обращении в полицию из-за долгого процесса и низкой вероятности успеха. В результате большинство дел о телефонном и интернет-мошенничестве прекращается на стадии предварительного расследования, а судебные иски часто остаются без удовлетворения.

Для улучшения противодействия преступлениям в сфере IT-технологий можно предложить следующие меры:

Укрепление кибербезопасности: внедрить в систему ГосСОПКА технологии резервирования каналов связи и географического распределения центров обработки данных с использованием облачных технологий. Это обеспечит единство критической информационной инфраструктуры и их независимость в случае кибератак, а также сохранность данных для расследования.

Интеграция правоохранительных органов: Подключить МВД России и СК РФ к системам ГосСОПКА, ФинЦЕРТ и НКЦКИ для обмена оперативной информацией о киберинцидентах. Это позволит эффективно взаимодействовать и расследовать преступления в сфере телекоммуникаций.

Профессиональная подготовка сотрудников: разработать программы обучения сотрудников ОВД и СК РФ для расследования компьютерных и киберпреступлений. Включить специализированные курсы в образовательные программы, учитывая современные реалии и криминогенную обстановку.

Технологическое оснащение: создать государственно-частное партнерство для оснащения МВД России и СК РФ современными компьютерными и информационными технологиями. Интегрировать отечественные разработки в деятельность правоохранительных органов для повышения их технической готовности.

Международное сотрудничество: развивать дипломатические инициативы для международного взаимодействия с БРИКС и ШОС в области кибербезопасности. Это включает информационный обмен, техническую и технологическую поддержку, а также совместные исследования и подготовку кадров.

Список литературы

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. – 2016. – № 50. – Ст. 7074.

2. Приказ МВД России от 29.12.2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

3. Министерство внутренних дел Российской Федерации: состояние преступности в Российской Федерации за январь–декабрь 2024 года: офиц. сайт. – URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 10.05.2025).

4. ФинЦЕРТ: структурное подразделение Банка России. URL: https://www.cbr.ru/information_security/fincert/.

5. Акапьев В. Л., Дрога А. А., Савотченко С. Е. Профилактика преступлений в сфере информационных технологий // Алтайский юридический вестник. – 2022. – № 4 (40). – С. 84–89.

6. Антонян Е. А., Бархатова Е. В. Противодействие киберпреступности // Евразийский Союз Ученых (ЕСУ). – 2019. – № 7 (64). – С. 54–57.

7. Кашкаров А. А. О некоторых особенностях предупреждения распространения информации экстремистской и иной деструктивной направленности в информационно-телекоммуникационных сетях, в том числе сети «Интернет» // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2019. – Т. 5, № 3. – С. 352–357.

8. Михайлова И. А., Лимарь А. С., Гилаев Р. И. О деятельности правоохранительных органов по противодействию преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий // ВЭПС. 2024. № 2. URL: <https://cyberleninka.ru/article/n/o-deyatelnosti-pravoohranitelnyh-organov-po-protivodeystviyu-prestupleniyam-sovershaemym-v-sfere-informatsionno> (дата обращения: 12.05.2025).

9. Яшин А. В., Фролова Т. А. Современные проблемы противодействия киберпреступлениям в Российской Федерации // Вестник Пензенского государственного университета. – 2023. – № 2. – С. 58–62.

10. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

11. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

12. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

13. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

14. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий :

Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYUOY.

15. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

16. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токотов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Крюченкова А. А.¹,
 курсант института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Поликарпова Е. В.,
 старший преподаватель
 кафедры противодействия преступлениям
 в сфере информационно-телекоммуникационных технологий
 Московского университета МВД России имени В.Я. Кикотя

ВОПРОСЫ ЗАЩИТЫ НЕСОВЕРШЕННОЛЕТНИХ ОТ КИБЕРБУЛЛИНГА

Информационно-телекоммуникационные технологии – это, несомненно, двигатель процесса во всех областях современного общества. Согласно отчету Digital 2024 Global Overview Report, в январе 2024 г. более 66 % всего населения Земли пользовалось всемирной сетью. Данный показатель увеличился на 1,8 % за 2023 г. [2].

Однако развитие доступных информационных технологий и вовлечение подростков и детей в цифровую среду становятся основными факторами риска для проявления девиантного поведения.

Кибербуллинг – одна из форм травли в сети Интернет, который приобретает свою особую опасность из-за анонимности и широкого охвата аудитории. Ни в России, ни на международном уровне не существует общепринятого определения «кибербуллинга». По мнению ЮНИСЕФ, «кибербуллинг – это буллинг с использованием цифровых технологий» [4].

Кибербуллинг может включать в себя распространение неловких фотографий, видео, унижительных комментариев, оскорбительных текстовых сообщений, публикаций в социальных сетях и т. д. Уровень кибербуллинга среди несовершеннолетних вызывает особую тревогу, так как может привести к стрессу, психологическим травмам и даже суицидальным мыслям. Так, в августе предыдущего года Алтайская самбистка трагически ушла из жизни в возрасте 17 лет. Как пишут СМИ, девушка оставила в своем телеграмм-канале публикацию с предсмертной запиской. «Я никогда не стыдилась своей национальности до тех пор, пока некоторые люди не стали превращать это в шутку» – говорится в сообщении. Друзья спортсменки считают, что именно травля со стороны интернет-пользователей стало причиной совершения ей данного поступка [3]. Кибербуллинг, заключающийся в доведении жертвы интернет-травли до самоубийства или в склонении к совершению самоубийства, влечет ответственность по ст.ст. 110–110.1 УК РФ.

¹ © Крюченкова А. А., 2025.

Таким образом, кибербуллинг – это серьезная проблема современности. Хотя и научные исследования предлагают множество профилактических мер для родителей и педагогов, исключить полностью риск травли невозможно. Однако предупредить увеличение числа девиантного поведения в Интернете возможно через комплексный подход, включающий действия и родителей, и учреждений, и государства, и самих цифровых платформ.

Во-первых, к сожалению, многие родители, сталкиваясь с кибербуллингом своих детей, считают, что это возможно решить, ограничив доступ ребенка к интернету. Однако – Интернет, это не только место для развлечений, но и огромный ресурс знаний и средств общения, необходимый для социализации. Родители должны строить взаимоотношения с детьми на доверии, чтобы последние могли без страха рассказать о проблемах в интернете. И если ребенок все-таки стал жертвой необходимо обратиться за помощью к психологу или другому специалисту.

Во-вторых, очевидно, что безопасность детей и подростков вызывает серьезную озабоченность и у политиков, как на национальном, так и международных уровнях. Что касается кибербуллинга, ряд законодательных инициатив сосредоточена на данном вопросе, начиная от Конвенции Организации Объединенных Наций о правах ребенка 1989 г. до Уголовного кодекса РФ. Уголовная ответственность за кибербуллинг может наступить в соответствии со ст.ст. 128.1 (клевета), 213 (хулиганство), 137 (нарушение неприкосновенности частной жизни), 138 (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений) УК РФ [1]. Отсутствие в уголовном законодательстве РФ специальной нормы, предусматривающей ответственность за кибербуллинг, как отдельное преступление, является, по нашему мнению, проблемой. С учетом многоаспектности кибербуллинга, его способов и направленности посягательств на различные общественные отношения создается необходимость принятия данной нормы в Уголовный кодекс РФ.

А также считаем, что можно внести изменения в ст. 137 УК РФ, дополнив норму частью 3 следующим содержанием:

«3. Те же деяния, совершенные лицом с использованием информационно-телекоммуникационной сети Интернет».

В-третьих, в школах и иных учреждениях должны проходить регулярные беседы и тренинги, посвященные предупреждению кибербуллинга. Важно не просто рассказать о данной проблематике, но и научить детей распознавать ситуации кибербуллинга, правильно реагировать на него и не бояться вовремя обращаться за помощью.

В-четвертых, сами цифровые платформы должны максимально обеспечивать эффективную модерацию контента, удаляя сообщения, содержащие элементы кибербуллинга.

Таким образом, только такой комплексный подход, объединяющий все усилия, может эффективно противостоять кибербуллингу и обеспечить безопасность несовершеннолетних в цифровой среде. Важно помнить, что именно профилактика и раннее выявление проблемы – первые шаги в борьбе с кибербуллингом.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) // Собрание законодательства РФ. 1996. №25. ст. 295.
2. Digital 2024: Global Overview Report // DataReportal .URL: <https://datareportal.com/reports/digital-2024-global-overview-report> (дата обращения: 13.01.2025).
3. URL: <https://sport24.ru/other/news-676085-na-altaye-17-letnyaya-sambistka-sovershila-suitsid-iz-za-travli-v-chem-moya-vina-v-tom-chto-rodilas-s-uzkimi-glazami?ysclid=m5wrkt1wa1215261276> (дата обращения: 13.01.2025).
4. URL: <https://www.unicef.org/end-violence/how-to-stop-cyberbullying> (дата обращения: 13.01.2025).
5. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
6. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.
7. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
8. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
9. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
10. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

Кубков М. А.¹,
*курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Токолов А. В.,
*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В КИБЕРБЕЗОПАСНОСТИ

В современном мире информационные технологии стали неотъемлемой частью повседневной жизни. Однако с ростом их значимости увеличивается и число угроз, связанных с киберпреступностью.

Что такое социальная инженерия? Социальная инженерия использует психологию человека, а не технические уязвимости. Это искусство манипулирования людьми, чтобы заставить их выдать конфиденциальную информацию или предпринять действия, которые ставят под угрозу безопасность, при этом они даже не подозревают, что их обманули. В отличие от хакерских атак на системы, социальная инженерия нацелена на людей. Злоумышленники используют такие черты, как доверие, страх, любопытство или инстинктивное желание помочь.

Убедительное электронное письмо от службы ИТ-поддержки с запросом ваших регистрационных данных? Это социальная инженерия в действии. Почему это так важно? Люди часто являются самым слабым звеном в кибербезопасности. Вот почему компании должны изменить фокус – не просто обеспечить безопасность систем, но и обучить сотрудников распознавать эти психологические уловки. Осведомленность и бдительность – это ваша первая линия обороны.

Социальная инженерия основывается на одной простой истине: людей взломать легче, чем системы.

Злоумышленники используют психологические приемы, чтобы манипулировать людьми, заставляя их раскрывать конфиденциальную информацию или предоставлять доступ к защищенным системам. Эти методы часто используют такие эмоции, как доверие, страх или любопытство, что делает их чрезвычайно эффективными.

Фишинг: поддельное электронное письмо от «службы технической поддержки» с просьбой сбросить пароль по вредоносной ссылке. Поддайтесь на это, и у злоумышленника будут ваши учетные данные.

¹ © Кубков М. А., 2025.

Pretexting (Претекст): злоумышленник придумывает правдоподобную историю, например, выдает себя за сотрудника вашего банка, чтобы «подтвердить» данные учетной записи, и убеждает вас поделиться личной информацией.

Baiting (Приманка): Заманчивая приманка, например, USB-накопитель с пометкой «Конфиденциально», оставленный в общем доступе. Если вы подключите его к своему компьютеру, это может привести к установке вредоносного ПО.

Перехват: незнакомец придерживает за вами дверь в защищенном офисе, рассчитывая на то, что вы из вежливости предоставите ему доступ, которого у него не должно быть.

Используя повседневные взаимодействия и поведение, социальная инженерия обходит брандмауэры

Почему социальная инженерия представляет угрозу для кибербезопасности? Самым слабым звеном в кибербезопасности является не программное обеспечение, а поведение человека.

Социальная инженерия представляет собой серьезную угрозу, поскольку она нацелена на людей, а не на системы. В то время как брандмауэры и антивирусное программное обеспечение защищают от технических уязвимостей, социальная инженерия обходит эти средства защиты, используя психологию человека. Злоумышленники манипулируют доверием, страхом или срочностью, чтобы обманом заставить людей раскрыть конфиденциальную информацию или предоставить доступ к защищенным системам.

В отличие от традиционного хакинга, который нацелен на взлом технологий, социальная инженерия опирается на принятие решений и эмоциональные реакции. Это делает ее особенно опасной, поскольку даже самые передовые технические средства защиты не могут полностью защитить от человеческих ошибок.

Для организаций проблема заключается в устранении этой уязвимости. Обучение сотрудников распознавать манипулятивные тактики и противостоять им имеет важное значение, но оно не является надежным. Человеческий фактор всегда будет объектом кибератак.

Атаки социальной инженерии могут нанести серьезный ущерб. Злоумышленники могут получить несанкционированный доступ к конфиденциальным данным, что приведет к утечкам, раскрывающим личную или корпоративную информацию. Финансовые потери также являются обычным явлением, будь то в результате мошенничества или обмана частных лиц при переводе денег. Для бизнеса последствия могут включать ущерб репутации, что затрудняет восстановление доверия клиентов и партнеров.

Эти атаки часто делают жертв более уязвимыми для будущих мошенников. Как только злоумышленники поймут, что их методы работают, они могут продолжать нападать на тех же людей или организации. Например, сотрудник, щелкнувший по фишинговому электронному письму, может случайно спровоцировать утечку данных, раскрыв конфиденциальную информацию о клиенте. Это не только наносит ущерб репутации компании, но также может привести к юридическим штрафам и проблемам с соблюдением требований законодательства.

В другом случае мошенник, использующий предлог, может выдавать себя за надежный источник, например, из ИТ-службы поддержки, и обманом вынудить сотрудника раскрыть регистрационные данные. Это показывает, как злоумышленники используют психологию человека – доверие, срочность и авторитет – для достижения своих целей.

Лучшей защитой можно назвать осведомленность и образование. Обучение сотрудников тому, как распознать эту тактику и соответствующим образом отреагировать, может иметь решающее значение для предотвращения потенциально разрушительных атак.

Таким образом, методы социальной инженерии являются одной из самых актуальных проблем в наше время и особенностью данной деятельности является воздействие не на ИТ-системы, а непосредственно на человека. Отсюда стоит обратить внимание на углубленное обучение людей для противодействия методам социальной инженерии и методам реакции на данный вид атак, то есть как человек должен поступать в той или иной ситуации.

Список литературы

1. Зотина Е. В. Претекстинг как прием социальной инженерии, используемый теле фонными мошенниками: криминологический взгляд на проблему // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50).
2. Костюхина Е. А. Разработка автоматической системы для обучения противодей ствию претекстингу // Проблемы правовой и технической защиты информации. 2022. № 10.
3. Михалева У. А. Претекстинг и способы противодействия ему // Вестник Даге станского государственного технического университета. Технические науки. 2023. Т. 50. № 2.
4. Рогожников А. С. Возможности социальной инженерии в информационной сфере // Современные информационные технологии: материалы IV Респ. с межд. уч. науч. интернет-конфер. студ., аспи р. и мол. уч. (21 мая 2021 г.). Донецк, 2021.
5. Самойлова А. А. Методы социальной инженерии // Тенденции развития науки и образования. 2019. № 56–3.
6. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
7. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
8. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
9. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва :

Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

10. Константинов А.В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

11. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Кудрявцев Д. А.¹,

курсант факультета подготовки сотрудников

для оперативных подразделений полиции

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Токолов А. В.,

доцент кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Современный мир находится в стадии постоянного развития, причем это развитие касается всех сфер жизни общества. Однако, по большей части, мир развивается в связи с высокими темпами развития науки, техники и, как следствие, высоким уровнем научно-технического прогресса. Речь идет о повсеместной информатизации общества – переводом осуществления его деятельности в режим «online», когда взаимодействие между людьми происходит посредством сети Интернет. Также, наравне с информатизацией общества происходит и процесс компьютеризации, связанный с приобщением различных групп населения к пользованию компьютерной техникой, а также сервисами сети Интернет.

Сфера услуг набирает обороты в своем применении, теперь, все больше людей работают не на промышленность, а на более интересные для них сферы деятельности. К примеру, возьмем наиболее распространенные профессии среди современных людей – педагог, юрист, маркетолог и так далее, замечу то, что все они связаны с предоставлением услуг. Так вот, с чем же связана информатизация?

Главной причиной является огромное количество бумажной информации, которая крайне неудобна для форматирования и систематизации, и, для облегчения работы с ней люди начали ее переводить в электронный вид. Также людям не комфортно работать в сфере услуг путем личных встреч, к примеру, оказание услуг юридических консультаций. Подумайте, хочется ли вам ехать куда-то в офис к юристу? Конечно же, каждый ответит, что нет, вот так думает и большинство людей. Поэтому многие организации переходят в режим предоставления услуг онлайн. А это значит, что нагрузка на информационные сети и их востребованность становится довольно высокой.

Следствием вышеописанных явлений является и перевод данных в электронный формат. Появление электронного документооборота, хранение данных на компьютере, пользование большинства граждан банковскими картами, наличие у всех граждан телефонов, а также другие факторы, способствуют и развитию

¹ © Кудрявцев Д. А., 2025.

преступности. Причем параллельно развивается большое количество видов новых преступлений. Зачастую, преступления, затрагивающие информационную сферу жизни общества, касаются следующего:

- неправомерного завладения конфиденциальной информацией физических, юридических, а также должностных лиц и организаций;
- воздействия на информационно-телекоммуникационные и компьютерные сети, посредством внедрения вирусного ПО;
- выведение из строя компьютерной техники граждан и организаций;
- хищение денежных средств со счетов;
- и так далее.

Как стало ясно, зачастую объектом посягательства преступников в информационной сфере является как раз-таки информация. К информации, которая интересна злоумышленникам можно отнести следующие виды:

- персональные данные;
- данные банковских карт;
- сведения, составляющие государственную, служебную или иную, защищаемую законом тайну;
- и другие.

Для реализации своих целей, злоумышленники могут использовать различные средства, и к таким средствам можно отнести как внедрение вредоносного ПО, распространение вредоносных ссылок или же создание сайтов клонов, так и методы, связанные с психологическим воздействием на личность потенциальной жертвы. И к последней группе методов относится социальная инженерия, направленная на заполучение необходимых злоумышленникам данных [2].

Сейчас социальная инженерия очень распространена среди преступлений, связанных с осуществлением мошеннической деятельности, что составляет, по данным МВД России на 2022 г., порядка 30 % от общего числа совершаемых на территории РФ преступлений. Такая цифра связана с тем, что гражданам очень сложно определить злоумышленника в интернете или по телефону, отсюда возникает большое количество списаний денежных средств с банковских счетов граждан.

Преступники постоянно усиливают свою материально-техническую базу и придумывают все новые и новые методы завладения чужими данными и денежными средствами. Причем сама преступность в данной сфере приобрела новый вид и стала именоваться киберпреступностью [1]. Для осуществления своих целей киберпреступники углубились в психологию и стали применять в своей деятельности методы социальной инженерии. Что это и как оно работает, а самое главное, как от нее защититься? Этому и посвящена данная научно-исследовательская работа.

Особую актуальность, на сегодняшний день представляет разработка теоретических положений о социальной инженерии, которые помогут гражданам избежать ее воздействия. Также, является необходимым определить направления совершенствования ОВД в сфере противодействия методам социальной инженерии.

Список литературы

1. Кызыханов А. А., Байрушин Ф. Т. «К вопросу о социальной инженерии» [Интернет-ресурс] Режим доступа: URL: <https://cyberleninka.ru/article/n/k-voprosu-o-sotsialnoy-inzhenerii#:~:text=Социальная%20инженерия%20-%20метод%20получения,данным%20и%20другим%20защищенным%20системам> (дата обращения: 08.05.2025 г.).
2. Тепляков С. П. «Социальная инженерия. Анализ и методы защиты» [Электронный ресурс] URL: <https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-analiz-i-metody-zaschity> (дата обращения: 08.05.2025 г.).
3. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
4. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.
5. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
6. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
7. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
8. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

Куксов В. А.¹,

слушатель факультета

подготовки сотрудников для оперативных подразделений полиции

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Пестрецов М. А.,

доцент кафедры

оперативно-разыскной деятельности и специальной техники

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ОТДЕЛЬНЫЕ ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ МЕЖДУНАРОДНОМУ ПРОЯВЛЕНИЮ ЭКСТРЕМИЗМА ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В СЕТИ ИНТЕРНЕТ

В современном мире Интернет стал не только платформой для свободного обмена информацией, но и ареной для распространения экстремистских идеологий. Органы внутренних дел (далее по тексту – ОВД) Российской Федерации (далее по тексту – РФ) сталкиваются с серьезной задачей – противодействие международному экстремизму в цифровом пространстве. Эффективное информационное противодействие требует комплексного подхода, включая анализ, превентивные меры и оперативное вмешательство.

Утвержденная Указом Президента Российской Федерации «Стратегия противодействия экстремизму в Российской Федерации» в п. 18 отмечает, что «Экстремистские и иные антиобщественные организации используют информационно-телекоммуникационные сети, включая сеть Интернет, мультимедийные и онлайн-технологии для вербовки новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии, а также финансирования экстремистской деятельности», подтверждая актуальность избранной для исследования тематики [1].

Информационное противодействие играет ключевую роль в противодействии международному экстремизму, особенно в условиях глобализации цифровых технологий. Оперативные подразделения ОВД РФ используют различные методы для мониторинга и анализа информационного пространства, что позволяет своевременно выявлять угрозы и принимать меры для их нейтрализации. Важным аспектом является сотрудничество на международном уровне, поскольку экстремистские группы часто действуют трансгранично. С. Д. Абакарова в своем исследовании отмечает, что взаимодействие правоохранительных органов по вопросам преступности в социальных сетях на современном этапе международных отношений находится в серьезном упадке [2]. Эффективное информационное

¹ © Куксов В. А., 2025.

противодействие предполагает не только блокировку экстремистских материалов, но и проведение превентивных информационных кампаний, направленных на противодействие идеологии экстремизма.

В рамках противодействия экстремизму в Интернете оперативные подразделения ОВД РФ применяют разнообразные методы и технологии. Значительное внимание уделяется мониторингу интернет-пространства с использованием автоматизированных систем, способных обрабатывать большие объемы данных. Эти системы помогают выявлять и анализировать экстремистские проявления, определять тенденции и связи между различными группировками.

К ключевым технологиям относятся алгоритмы глубокого обучения и текстовый анализ, которые позволяют распознавать запрещенную символику, сленг и другие индикаторы экстремистской деятельности в сети. Эффективное использование этих инструментов требует постоянного обновления и адаптации под современные вызовы, возникающие в связи с постоянным развитием цифровых технологий и изменениями в методах ведения деятельности экстремистов. Проактивное информационное взаимодействие с другими странами также играет важную роль в обмене опытом и данных, что усиливает общую эффективность противодействия экстремизму на международном уровне.

Оперативные подразделения ОВД РФ применяют комплексные методы противодействия проявлениям экстремизма в Интернете, что позволяет существенно повысить эффективность информационного противодействия. Используя современные технологии анализа данных и мониторинга социальных сетей, они оперативно выявляют и пресекают деятельность экстремистских группировок. Значительную роль играет сотрудничество с международными организациями и правоохранительными структурами других государств, что позволяет обмениваться опытом и информацией о новых методиках и подходах в данной области. Также акцент на обучение и повышение квалификации сотрудников увеличивает их способность адаптироваться к быстро меняющейся информационной среде и эффективно противостоять международному экстремизму [3].

Оперативные подразделения ОВД РФ активно интегрируют информационное противодействие в борьбу с международным экстремизмом в Интернете. Это включает в себя мониторинг социальных сетей, форумов и других платформ, на которых могут распространяться экстремистские идеи. Особое внимание уделяется анализу информационных потоков, позволяющему выявлять и пресекать попытки внешнего влияния на внутригосударственные процессы. Такая деятельность включает в себя использование современных технологий обработки данных, в том числе искусственного интеллекта для фильтрации и анализа больших объемов информации. Эффективность таких мер подтверждается успешными операциями по выявлению и блокированию экстремистских ячеек и их ресурсов в сети.

В перспективе развития мер по противодействию международному экстремизму в Интернете важную роль будет играть совершенствование технологий мониторинга и анализа данных. ОВД РФ планируют углублять сотрудничество с международными платформами для обмена опытом и технологиями. Также

предполагается использование искусственного интеллекта для оперативного выявления и блокирования контента экстремистской направленности. Усиление международного диалога по вопросам кибербезопасности и разработка общих подходов к регулированию информационного пространства помогут формировать более эффективные механизмы противодействия угрозам. Эти меры направлены на укрепление правопорядка и стабильности в обществе.

Список литературы

1. Указ Президента Российской Федерации от 28 декабря 2024 г. № 1124 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации» // информационно-правовой портал «Гарант.ру».

2. Абакарова С. Д. Преступность в социальных сетях как угроза общественной безопасности / С. Д. Абакарова // Инновационный потенциал развития науки в современном мире: достижения и инновации : Сборник научных статей по материалам XVI Международной научно-практической конференции, Уфа, 28 января 2025 г. – Уфа: Общество с ограниченной ответственностью «Научно-издательский центр "Вестник науки"», 2025. – С. 207–212.

3. Порватова Л. В. Проблема международного терроризма: пути решения проблемы / Л. В. Порватова, В. А. Куксов // Правопорядок в России: проблемы совершенствования: XV Всероссийская конференция: сборник статей, Москва, 15–19 марта 2021 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2021. – С. 257–261.

Кузовлева М. А.¹,
 заместитель командира взвода
 института подготовки сотрудников
 для органов предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
 заместитель начальника кафедры противодействия преступлениям
 в сфере информационно-телекоммуникационных технологий
 Московского университета МВД России имени В.Я. Кикотя,
 кандидат юридических наук, доцент

ПРОФИЛАКТИКА ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

Органы внутренних дел ежедневно осуществляют борьбу с различными формами преступности, тем самым защищая граждан от преступных посягательств на их права и законные интересы. В настоящее время одним из актуальных вопросов в рамках борьбы с преступностью является противодействие мошенническим действиям, совершаемым дистанционным путем. Суть данных преступлений проста – хищение денежных средств граждан путем обмана. В рамках данной статьи мы рассмотрим наиболее перспективные, по нашему мнению, направления профилактической работы МВД России в сфере борьбы с мошенничеством.

Так, прежде чем мы перейдем к рассмотрению направлений деятельности подразделений МВД России по профилактике преступлений мошеннического характера, нам необходимо определиться с тем, что из себя представляет типичное дистанционное мошенничество. Обратившись к правоприменительной практике, мы заметим, что в настоящее время весьма распространена следующие схемы совершения мошенничества [3, с. 119–140]:

1. Осуществление звонка потенциальной жертве от лица правоохранительных органов либо финансово-кредитной организации – при реализации данного способа, злоумышленники используют номера телефонов, которые они получают из баз данных операторов связи и других источников (зачастую подобная информация приобретается в даркнете). Сущность данного способа заключается в том, чтобы посредством приемов социальной инженерии убедить жертву в том, что ее денежным средствам (банковским счетам) что-либо угрожает (блокировка либо попытка списания денежных средств), затем, после того как потенциальная жертва будет убеждена в том, что ее денежные средства находятся в опасности, злоумышленники убеждают ее перевести деньги на другой «защищенный» банковский счет, для обеспечения сохранности денежных средств. В результате подобного перевода жертва фактически самостоятельно отдает денежные средства

¹ © Кузовлева М. А., 2025.

злоумышленникам. Сложность раскрытия и расследования данных преступлений обуславливается тем, что СИМ-карты, посредством которых осуществляется звонок, не зарегистрированы на конкретного человека, либо зарегистрированы по подложным документам, а также тем, что счета на которые поступают денежные средства, полученные преступным путем, зарегистрированы в офшорных зонах, что, в свою очередь, делает невозможным получение какой либо информации о владельце счета, а также о количестве денежных средств, хранящихся на данном счете.

2. Рассылка СМС-сообщений, содержащих в себе ссылки на фишинговые сайты – в данном случае мы можем видеть синтез использования двух технологий: технологий мобильной связи и IT-технологий. Так, мобильная связь используется для массовой рассылки сообщений со ссылками на фишинговые сайты. После того как жертва преступления переходит по данной ссылке, ей предлагается ввести определенные личные данные (ФИО, паспортные данные, номера банковских карт и CVС коды). Данная информация получается под влиянием обмана или злоупотребления доверием (например, обещания крупного выигрыша, либо выгодных условий кредитования). После предоставления данной информации с банковских карт происходит списание денежных средств. Также, достаточно часто посредством подобных сайтов происходит распространение вредоносных программ на мобильные устройства граждан. Данные вредоносные программы могут выполнять различные функции, например, сбор информации о паролях и логинах, вводимых пользователем в банковских приложениях, после чего, злоумышленник удаленно получает доступ ко всем банковским картам пользователя и осуществляет списание денежных средств с банковской карты. В данном случае, помимо названных ранее сложностей, раскрытия подобных преступлений, появляется еще одна - позднее обнаружение потерпевшим пропажи денежных средств с банковской карты, в результате чего утрачиваются значимые следы преступления [3, с. 150–170].

3. Использование программ для переадресации вызова – зачастую преступники могут использовать специальные программы, которые позволяют осуществить переадресацию вызова мобильного устройства. В результате таких действий лицо может получить сообщение либо звонок со знакомого мобильного номера с просьбой прислать определенную сумму денежных средств. Данный способ крайне распространен по причине того, что выяснить реальный адрес или другие данные лица, осуществляющего звонок практически невозможно. Другой формой использования технологии переадресации вызова является установление на мобильное устройство потенциальной жертвы такой программы. Установка происходит дистанционно посредством заражения устройства вредоносными файлами. После чего вся та информация, которая сообщается лицом в СМС - сообщениях или личных звонках становится доступной для преступника. Таким образом злоумышленник может получить доступ не только к банковским приложениям, но и к электронному почтовому ящику, а также социальным сетям жертвы, в результате чего перед злоумышленником открывается большое количество возможностей для завладения денежными средствами жертвы.

Рассмотрим типичный пример совершения дистанционного мошенничества:

15.02.2025 в 13:00 года потерпевшей А. поступил звонок на мобильный телефон. Звонивший представился сотрудником центрального банка, и сообщил, что банковские счета А. находятся под угрозой блокировки из-за кибер атак на сервера банка и единственным способом спасти денежные средства являются снятие денежных средств со счетов и перевод их по тем реквизитам, которые укажет человек, назвавшийся Фоминым Алексеем Михайловичем (далее – Алексей).

После чего, Алексей предложил потерпевшей А. перейти для общения в WhatsApp, а также дал указание снимать денежные средства со счета и присылать ему фотографии денежных средств и чеков, подтверждающих саму операцию. Далее на скриншотах экрана потерпевшей мы увидим диалог, между Алексеем и потерпевшей.

Подобные действия со стороны преступника можно характеризовать с позиции психологии, как попытка взятия человека под контроль под влиянием страха, т. е. Алексей представился сотрудником достаточно серьезного государственного учреждения (для многих граждан истинная функция центрального банка не известна и не понятна), а затем сообщил, что денежные средства гражданина находятся под угрозой блокировки. Первая естественная реакция человека в такой ситуации – страх. Далее Алексей сообщает, что необходимо осуществить снятие денежных средств со счета, а также сделать фотографии денежных средств и чеков операции.

Подобные требования тоже играют определенную роль в механизме преступления. Так, требование обналичить все деньги не вызывает у жертвы каких-либо подозрений, поскольку сами деньги все еще находятся у нее, а просьба делать фотографии чеков придает данной ситуации определенный официальный вид, что в свою очередь также направлено на установление доверительного контакта с жертвой.

После того, как А. начала снимать денежные средства со своего счета, Алексей начал торопить А. тем самым, не давая ей времени на обдумывание всей ситуации и анализа происходящего

Далее мы можем видеть, как Алексей совершает ряд попыток дозвониться до А. тем самым поторопив ее. Данные действия, как и предыдущие направлены на создание паники у потенциальной жертвы, и убеждения ее в необходимости совершения скорейших действий по снятию денежных средств со своего банковского счета.

Далее Алексей вновь позвонил А. и сообщил, что она должна зарегистрироваться в банковском приложении, и оформить на себя банковскую карту, что впоследствии А. и сделала.

После того, как А. оформила банковскую карту, Алексей вновь потребовал фото подтверждение снятия денежных средств со счета, а также купить новую СИМ-карту на свое имя.

Поскольку на банковском счету А. находилась сумма денежных средств в размере 900 000 рублей, то снять ее за один раз не представлялось возможным, о чем А. сообщила Алексею позвонив ему. Алексей пояснил, что снять деньги можно в разных терминалах, и это не является критичным. После этого Алексей сказал, что А. необходимо приобрести мобильный телефон определенной модели.

Подобные действия необходимы Алексею в целях дистанционного установления на данный телефон вредоносных программ, дающих дистанционный доступ к мобильному устройству. Конкретная модель телефона была выбрана из-за существующих системных «дыр» в программном обеспечении данной модели.

После того, как А. сняла все имеющиеся деньги с банковского счета, она позвонила Алексею и сообщила об этом. После чего Алексей сообщил ей, что появилась возможность поместить ее денежные средства на «особый» банковский счет с очень высокими процентами. В целях удостоверить А. в правдивости своих слов Алексей прислал ей скан документа, удостоверяющего личность сотрудника центрального банка. После того, как А. убедилась в подлинности обещаний Алексея, она вновь вернула денежные средства на банковскую карту, оформленную ранее, и осуществила перевод денежных средств на реквизиты, которые указал Алексей, в сумме А. отправила на указанный счет 600 000 рублей. В целях подтверждения защиты денежных средств А. Алексей сообщил ей, что с А. должен связаться сотрудник ФСБ России, и прислать ей соответствующие документы.

Сотрудник ФСБ России действительно связался с А. посредством мессенджера Telegram, где сообщил А., что ее документы на открытие счета с повышенной процентной ставкой действительно поступили в работу. Для подтверждения факта работы в ФСБ России данный гражданин сделал фото служебного удостоверения, которое по форме и содержанию не похоже ни на один из существующих образцов служебных документов органов исполнительной власти России.

После перевода половины тех денежных средств, которые А. сняла со своих сберегательных счетов, потерпевшая начала сомневаться в совершаемых действиях, и рассказала своему молодому человеку о всех своих действиях, после чего прекратила общение со злоумышленниками, однако Алексей начал попытки связаться с А., а также попытался убедить ее продолжить перевод денежных средств по указанным ранее реквизитам, обещав дать доступ к личному кабинету (сайту, сделанному по образу сайта Сбербанка, где отображалась перечисленная сумма). Функционал сайта был ограничен, а также URL ссылка отображалась не корректно, что и дало А. основания полагать, что в отношении нее были совершены мошеннические действия.

После того, как А. осознала факт обмана, она сообщила о произошедшем в полицию, где по факту заявления была начата проверка, в результате которой было возбуждено уголовное дело по ч. 2 ст. 159.3 УК РФ.

Рассмотренный нами пример реальной практической ситуации наглядно демонстрирует как преступники в целях реализации своего умысла комбинируют сотовую связь (посредством которой происходило первоначальное общение с потенциальной жертвой, а также осуществлялась координация действий потерпевшей), приемы социальной инженерии, а также современные информационные технологии. В совокупности данные методы позволяют злоумышленникам получать доступ к денежным средствам граждан.

Исходя из механизма совершения рассматриваемого преступления, мы можем определить и механизм противодействия. МВД России, как правоохранительный

орган ведет активную деятельность, направленную на информирование населения об угрозах, связанных с дистанционными мошенничествами. Информирование ведется в основном путем личных бесед участковых с гражданами, в отношении которых уже совершены мошеннические действия. По нашему мнению, подобная позиция не правильная. Для повышения уровня информированности граждан о подобного рода преступлениях необходимо:

1. Проведение МВД России в инициативном порядке интернет-компаний, информирующей граждан о возможных угрозах со стороны мошенников. Так, в данную компанию могут включаться – рассылка сообщений с предупреждениями на личную почту или на мобильные устройства, размещение рекламы на сайтах с предупреждениями о мошеннических действиях, блокировка подозрительных интернет-ресурсов (данное действие должно проводится при участии Роскомнадзора).

2. Проведение лекций в образовательных учреждениях, о системе правоохранительных органах, их функциях и задачах, с целью уяснения гражданами сведений о том, что сотрудники правоохранительных органов не будут самостоятельно связываться с гражданами РФ и вести разговор об их денежных средствах.

3. Проведение открытых встреч сотрудников полиции с наиболее уязвимыми слоями населения (пенсионерами), с целью проведения профилактических бесед об угрозе мошеннических действий.

4. Размещение вблизи банкоматов предупреждающих плакатов об опасности мошеннических действий. Так, в настоящее время подобные плакаты стали появляться на улицах некоторых городов, однако в силу того, что на данных плакатах используются цвета из геральдики МВД России – синий, белый или желтый, то данные плакаты на подсознательном уровне игнорируются нашим мозгом, а, следовательно, представленная там информация не усваивается гражданами. Для исправления данной ситуации необходимо издание новых плакатов в других цветовых решениях, например, красном цвете, или ярко желтом, с целью привлечения внимания к ним.

Подводя итог изложенному выше, мы можем сделать вывод о том, что в настоящее время дистанционное мошенничество действительно является одним из самых распространенных составов преступлений, совершаемых в нашей стране. Ежегодный ущерб от данного вида преступной деятельности исчисляется миллиардами рублей. По нашему мнению, причиной такой распространенности данного состава преступления является неосведомленность большинства наших сограждан о принципах деятельности тех или иных органов государственной власти, их целях, задачах и полномочиях, в результате чего у мошенников появляется возможность внушить таким гражданам свои ложные истории, в результате которых граждане теряют свои денежные средства. Единственным возможным способом противодействия таким преступлениям является профилактика. В настоящее время МВД России ведет активную деятельность в данном направлении, однако не все аспекты современной жизни затронуты такой профилактикой. В рамках данной статьи мы привели некоторые примеры совершенствования сло-

жившейся в настоящее время практики по профилактике подобных преступлений. По нашему мнению, в случае успешного внедрения указанных приемов эффективность профилактических мероприятий можеткратно возрасти.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025).
3. Гладкий А. Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников / Алексей Гладкий. – М.: АВТОР, 2021. – 161 с.
4. Зыков Д. А. Компьютерное мошенничество: / Даниил Алексеевич Зыков. – М.: LAP Lambert Academic Publishing, 2022. – 188 с.
5. Иван, Фойницкий Мошенничество по русскому праву. В 2 частях (количество томов: 2) / Фойницкий Иван. – М.: Современный гуманитарный университет (СГУ), 2021. – 457 с.
5. Как не стать жертвой преступления, мошенничества и обмана. – М.: Текарт, 2023. – 288 с.
6. Клим Максим. Как уберечь себя от действий мошенников. Мануал. Как избежать мошенничества / Максим Клим. – М.: Издательские решения, 2020. – 635 с.
7. Кузько Е. С. Мошенничество в сфере страхования. Уголовно-правовая характеристика и практика квалификации: монография / Е. С. Кузько. – М.: КноРус, 2021. – 120 с.
8. Михайловская Ю. В. Мошенничество и его профилактика / Ю. В. Михайловская. – Москва: Огни, 2023. – 903 с.
9. Мошенничество в платежной сфере. Бизнес-энциклопедия. – М.: Интеллектуальная Литература, 2020. – 231 с.
10. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В.Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
11. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
12. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
13. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

14. Стащенко С. П. К вопросу о классификации прав граждан в информационной сфере / С. П. Стащенко, А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 5. – С. 219–222. – DOI 10.24412/2073-0454-2023-5-219-222. – EDN TUUOVO.

Лисица А. А.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России им. В.Я. Кикотя*

Научный руководитель:

Харламова И. Ю.,

*доцент кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, доцент*

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРБУЛЛИНГА

В современном мире в человека и общества в целом активно внедряются различные информационные технологии, которые значительно упрощают выполнение работы, позволяя быстро и качественно выполнить ее. Однако развитие цифровых технологий порождает новые виды киберпреступлений, среди них наиболее распространенным является кибербуллинг. Впервые данное понятие ввел Билл Белси.

Кибербуллинг – это использование информационных и коммуникационных технологий, например, электронной почты, мобильного телефона, личных интернет-сайтов, для намеренного, неоднократного и враждебного поведения лица или группы, направленного на оскорбление других людей. В процессе общения в интернете теряют свое значение коммуникативные преграды, существующие в реальной жизни. Все действия совершаются с использованием сообщений в мессенджерах и социальных сетях, а также посредством выкладывания фотографий и видеоматериалов, содержащих порочащую для репутации жертвы информацию в сети Интернет.

Статья направлена на выявление тенденций развития кибербуллинга в современном мире.

Люди, подвергающиеся кибербуллингу, часто оказываются в более сложной ситуации, чем жертвы обычной травли. Постоянное преследование в интернете, не ограниченное временем и местом, делает их особенно уязвимыми. Это может приводить к нежеланию учиться и глубоким изменениям в личности. Исходя из данных статистики, которая указывает на то, что случаи кибербуллинга увеличились на 68,5 % в сравнении с прошлыми годами, можно сделать вывод о том, что данная проблема является наиболее актуальной и распространенной как среди молодежи, так и более взрослого поколения. В группу риска попали следующие категории населения:

1. Дети и подростки (особенно в закрытых школьных чатах).
2. Женщины и девушки, подвергающиеся сексуализированным угрозам, доксингу.
3. Блогеры и публичные личности (негативные комментарии, угрозы).

¹ © Лисица А. А., 2025.

Нередки случаи кибербуллинга и среди ЛГБТ-сообществ, которые подвергаются травле в различных интернет-форумах.

Почему же случаи кибербуллинга становятся все более распространенными? Причин несколько.

Во-первых, подобные преступления совершают те, кто лишен чувства эмпатии. Снижение эмпатии же связывают с тем, что люди все чаще предпочитают живому общению виртуальное. Такие люди не умеют сочувствовать другим и не осознают, какой вред наносят своими поступками. Унижая жертву, они чувствуют силу [1]. Гораздо проще совершать преступления в интернете, ведь чаще всего ответственность за них не наступает.

Во-вторых, отсутствие родительского внимания приводит к тому, что ребенок, пытаясь унять агрессию, не говорит об этом своей семье, а выплескивает ее на других людях [2]. Они становятся активными участниками различных групп и чатов, где унижать жертву становится привычным занятием.

К современным тенденциям развития кибербуллинга относятся:

1. Появление новых интернет-платформ.

- Tik-Tok и иные приложения для просмотра коротких видеороликов, в которых пользователи, выкладывая контент, активно подвергаются унижению со стороны зрителей;

- игровые чаты (Twitch, Discord), в которых происходит буллинг в кооперативных играх, а также унижения со стороны других игроков;

- Telegram-каналы и чаты. В них могут создаваться анонимные чаты для травли различных пользователей;

- анонимные приложения, в которых активно распространяется дезинформация о человеке и его жизни.

2. Искусственный интеллект и deepfake.

- Deepfake-буллинг, с помощью которых создаются и распространяются фото и видео жертвы в непристойных и унижительных ситуациях;

- боты и нейросети – автоматизированные атаки через массовые оскорбительные комментарии;

- голосовой кибербуллинг, который использует клонирует голос жертвы для создания фейковых аудио с компрометирующими фразами.

3. Кибербуллинг в метавселенных и VR.

- виртуальные оскорбления, домогательства в Meta Horizon Worlds, VRChat;

- создание аватаров-жертв для публичных унижений.

4. Доксинг и цифровой шантаж.

- утечка личных данных (адреса, номера телефонов, фото личного характера);

- шантаж с угрозой публикации компромата.

5. Организованный кибермобин.

- координированные атаки групп агрессоров, к которым относятся рейды в социальных сетях;

- флешмоб с хештегами для травли.

Все эти тенденции указывают на то, что кибербуллинг преследует жертву не только в конкретной социальной сети, а в сети Интернет в целом.

Кибербуллинг значительно влияет на психологическое состояние личности. Жертва, подверженная такому типу буллинга, становится более уязвимой для новых угроз.

К основным последствиям кибербуллинга можно отнести следующие:

1. Изменения человека в поведении в результате кибербуллинга, к которым можно отнести:

- становится более тихим и отрешенным;
- теряет интерес к любимым занятиям;
- частые перепады настроения;
- старается не пользоваться телефоном;
- становится озлобленным;
- появляются мысли о суициде и др.

Кибербуллинг разрушает жизнь человека. Жертвы испытывают мучительную тревогу, впадают в депрессию, теряют уверенность в себе и могут даже проявлять агрессию. Эмоциональная боль, причиненная онлайн-травлей, может быть настолько сильной, что требует длительной психотерапии [3]. Постоянное ощущение, что унижительные материалы доступны для всеобщего обозрения, вызывает у жертвы чувство стыда и незащищенности, погружая ее в состояние непрекращающегося стресса.

2. Помимо психологических изменений в поведении человека также наблюдаются и физические изменения, которые проявляются в следующем:

- сильный стресс и тревожность, которые могут привести к бессоннице и проблемам с пищеварением;
- снижение двигательной активности в целом.

Кибербуллинг – страшное преступление против личности, с последствиями которых часто не могут справиться даже взрослые и осознанные люди. Что касается молодежи, которая в силу своего возраста отличается неустойчивой психикой и зачастую заканчивают жизнь из-за различной травли в интернет-пространстве, то для людей, относящихся к этой социальной группе необходим особый подход.

Вот некоторые методы борьбы и профилактики кибербуллинга:

1. Технические способы защиты, к которым относятся:

- блокировка агрессоров, настройки приватности;
- использование VPN и анонимных аккаунтов;
- мониторинг цифрового следа.

2. Правовые меры

- обращение в поддержку социальных сетей;
- заявление в полицию;
- иски о компенсации морального вреда.

3. Психологические меры

- предоставление бесплатного психолога жертвам кибербуллинга;
- службы поддержки.

Совокупность мер позволяет сохранить психическое и физическое здоровье жертвы, обеспечить ее безопасность и постараться не допустить повторного совершения подобного преступления.

Таким образом, кибербуллинг является наиболее распространенной и опасной формой совершения преступления в современном мире. Исходя из российского законодательства, в котором прописано, что в скором времени информационные технологии в ближайшем времени должны стать неотъемлемой частью жизни общества, в законы требуется внести поправки о безопасном использовании сети Интернет. Необходимо создать нормативную базу, которая сможет защитить пользователей от кибербуллинга и не допустить совершения новых преступлений в данной сфере. Это нужно для того, чтобы каждый пользователь чувствовал себя комфортно, пользуясь различными сайтами и приложениями. В этом помогут различные тренинги, на которых будут подробно объяснены правила пользования интернетом, а также вред, наносимый жертве, подвергшейся кибербуллингу. Если каждый пользователь будет использовать информационные технологии в благих целях, преступлений в этой сфере станет в разы меньше, а люди начнут себя более комфортно чувствовать в информационном пространстве.

Список литературы

1. Официальный сайт «Парламентской газеты» (Издание Федерального Собрания Российской Федерации). URL: <https://www.pnp.ru/social/zakiberbulling-predlagayut-vvestiugolovnoe-nakazanie.html> (дата обращения: 10.05.2025).
2. Официальный сайт Института изучения детства, семьи и воспитания. URL: <https://институтвоспитания.рф/press-center/news/11-noyabrya-otmechaetsya-den-borby-s-kiberbullingom/?ysclid=ltu49rb97i716828911> (дата обращения: 09.05.2025).
3. Газизьянов Т. А., Мансурова З. Р. Психология кибербуллинга. Виды и причины кибербуллинга // Общество, право, государственность: ретроспектива и перспектива. 2023. № 4 (16). С. 89–92.
4. Бородина В. Н. Роль детско-родительских отношений в возникновении кибербуллинга // Мир науки, культуры, образования. 2023. № 1 (98). С. 138–141.
5. Официальный сайт интернет-издания mk-turkey.ru. URL: <https://mkturkey.ru/education/2023/11/30/pministerstvoobrazovaniyavklyuchiloizucheniiekiberzapugivanievuchebnuyuprogrammuturcii.html?ysclid=ltyio99hl651315742> (дата обращения: 10.05.2024).

Лукашенко П. П.¹,
курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Рудин А. В.,
доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

МЕТОДИКА РАССЛЕДОВАНИЯ ДИСТАНЦИОННЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, НА ОНЛАЙН-ПЛАТФОРМАХ ДЛЯ РАЗМЕЩЕНИЯ ОБЪЯВЛЕНИЙ

В современной России активно реализуется информатизация, пронизывающая все сферы жизнедеятельности – государственное управление, экономику, социальную сферу и повседневную жизнь граждан на основе комплекса нормативно-правовых актов. Информационные технологии становятся ключевым фактором повышения эффективности работы органов власти, бизнеса и систем социального обеспечения. Конституция Российской Федерации закрепляет право каждого на свободный поиск, получение, передачу, производство и распространение информации любым законным способом, что создает конституционные гарантии развития информационного общества. Информационные технологии проникают в производственные процессы, логистику и коммерцию. Одним из примеров может стать появление онлайн-платформ для размещения объявлений (доски объявлений).

В современной медиасреде онлайн-платформы для размещения объявлений стали одним из основных каналов коммуникации между продавцами и покупателями. Их ключевыми преимуществами являются широкий охват аудитории, экономичность и оперативность – они позволяют быстро и дешево найти интересующую аудиторию. При этом существуют и значимые риски. Наиболее значимой опасностью является отсутствие надежной модерации, что порождает размещение фальшивых объявлений, и как следствие – совершение преступных действий в данной сфере.

В последние годы число преступлений, совершаемых через онлайн-платформы для размещения объявлений, резко возросло. По данным МВД России,

¹ © Лукашенко П. П., 2025.

«виртуальные мошенничества» уже составляют около 40 % от всех зарегистрированных преступлений в России, значительная доля из которых приходится на доски объявлений «Авито» и «Юла». Ежегодный оборот ущерба от мошенничества на сервисах объявлений оценивается в сумму до 1 млрд рублей. Роскомнадзор и правоохранительные органы фиксируют сотни тысяч инцидентов: так, только за 2023 г. число интернет-преступлений увеличилось на 29,7 %, достигнув 677 000 случаев [3].

К числу таких преступлений относятся мошенничества, кражи с использованием поддельных ссылок, неправомерный доступ к аккаунтам и др. Основные характеристики: анонимность субъектов; мобильность преступников; использование поддельных документов и учетных записей; усложненный механизм идентификации участников. Преступник может создать фальшивое объявление, предложить вымышленный товар и получить предоплату, не намереваясь выполнять установленные ранее обязательства.

Рассмотрим методику расследования дистанционных преступлений на основе интернет-платформы «Авито».

В ходе проведения доследственной проверки по факту возможного преступления осуществляется всестороннее изучение всех доступных данных, полученных из различных источников. Первоочередное внимание уделяется анализу электронных сообщений, фото- и видеоматериалов, а также иных цифровых носителей, которые могут содержать сведения, подтверждающие наличие признаков противоправной деятельности. Параллельно проводится мониторинг активности на серверах, осуществляется сбор данных о действиях пользователей в сети Интернет, а при необходимости обеспечивается доступ к содержимому электронных почтовых ящиков и учетных записей в социальных сетях.

После официального возбуждения уголовного дела по факту преступления, совершенного с использованием информационно-телекоммуникационных технологий, следователь, руководствуясь положениями Уголовно-процессуального кодекса Российской Федерации, выполняет следующие процессуальные действия:

1. Признание потерпевшего и его допрос. Следователь выносит процессуальное решение о признании лица, которому причинен материальный ущерб, потерпевшим, и проводит его допрос в соответствии с положениями частей 2–6 статьи 278 и статьи 278.1 Уголовно-процессуального кодекса Российской Федерации.

2. Установление лиц, осуществивших денежные переводы. Производится идентификация номеров телефонов лиц, осуществивших переводы денежных средств на банковский счет, использованный в рамках противоправной схемы. Далее направляются официальные запросы с целью установления их фактического местонахождения.

3. Вызов свидетелей. После установления контактных данных указанных лиц им направляются повестки с требованием явки в следственные органы для дачи показаний в качестве свидетелей.

4. Признание новых потерпевших. В случае, если свидетель подтверждает факт причинения материального ущерба, его показания и материалы проверки

приобщаются к основному уголовному делу. Свидетель также официально признается потерпевшим, что способствует оптимизации процесса расследования и оперативной защите прав пострадавших.

Таким образом, на первоначальном этапе расследования преступлений, совершенных с использованием дистанционных технологий, ключевыми задачами являются детальный анализ цифровых следов, своевременное процессуальное оформление статуса потерпевшего, выявление и вызов свидетелей, а также обеспечение надлежащего документального оформления собранных доказательств.

В процессе расследования преступлений, связанных с использованием информационных и коммуникационных технологий, включая платформу «Авито», правоохранительные органы проводят комплекс мероприятий по сбору и анализу цифровых следов. Первоначально осуществляется запрос к администрации платформы с требованием предоставить информацию о сетевых адресах (IP-адресах), которые использовались для авторизации на сайте и размещения объявлений. Параллельно направляются запросы к интернет-провайдерам, обслуживающим указанные IP-адреса. Это позволяет определить географическое расположение устройств, с которых осуществлялись противоправные действия. На основании полученных данных проводится дальнейшая следственная работа, направленная на установление личности пользователя и его причастности к совершенному преступлению.

В случаях дистанционного мошенничества с использованием банковских карт сотрудники правоохранительных органов обращаются в банк-эмитент для получения детализированной информации о банковском счете, на который были перечислены средства за товар. Злоумышленники часто используют анонимные платежные инструменты, такие как виртуальные карты, например, до 2024 г. большой популярностью пользовалась платежная система Qiwi, (в феврале 2024 г. Центральный банк РФ отозвал лицензию у QIWI банка), которые регистрируются на телефонные номера, не всегда принадлежащие фактическому преступнику. Однако при прохождении процедуры верификации через паспортные данные в платежной системе удастся установить конечного владельца карты или электронного кошелька. Запрос в Бюро специальных технических мероприятий МВД России (БСТМ) позволяет получить информацию о технических устройствах, используемых для доступа к платформе «Авито», а также дополнительные сведения о пользователе. Данные операторов мобильной связи способствуют идентификации абонента по номеру телефона, указанному в объявлении, так как при подключении SIM-карты оператор фиксирует паспортные данные клиента.

После вынесения судебного постановления следователи обращаются к операторам связи с запросом о предоставлении информации о входящих и исходящих соединениях, связанных с конкретными абонентскими номерами и устройствами. Это позволяет реконструировать схему дистанционного мошенничества и установить все обстоятельства совершенного преступления.

Сотрудники правоохранительных органов осуществляют сбор информации о физических лицах, потенциально причастных к совершению преступления. В частности, анализируются данные о владельцах банковских карт, осуществляющих операции снятия наличных денежных средств через банкоматы, а также о

лицах, осуществляющих отправку и получение денежных переводов через почтовые отделения. Параллельно с этим проводятся обыски по месту жительства подозреваемого и его предполагаемых сообщников. На основании собранных доказательств осуществляется допрос подозреваемого. Также производится изъятие устройств, с которых осуществлялись мошеннические операции, с целью последующего их исследования.

В случае вынесения судом постановления о проведении осмотра сетевых ресурсов осуществляются соответствующие следственные мероприятия. Эти мероприятия могут включать в себя перехват интернет-трафика, установку программного обеспечения для удаленного доступа, а также обыск и изъятие компьютерной техники и других цифровых носителей информации.

Согласно ч. 6 ст. 164 Уголовно-процессуального кодекса Российской Федерации, в процессе проведения указанных действий допускается использование технических средств и методов, направленных на обнаружение, фиксацию и изъятие следов преступления и вещественных доказательств. В процессе анализа информационных ресурсов, размещенных в сети Интернет, уполномоченные органы, включая следственные и оперативные подразделения, применяют широкий спектр технических средств и программных комплексов. К таким инструментам относятся специализированное программное обеспечение для анализа цифровых данных, а также технологии удаленного доступа к электронным устройствам, потенциально использованным для совершения противоправных действий. Для защиты данных, полученных в ходе следственных мероприятий, от несанкционированного доступа и распространения применяются меры информационной безопасности. Кроме того, используются утилиты и оборудование для восстановления удаленных данных, анализа физических носителей информации, включая жесткие диски, и извлечения из них значимой для следствия информации.

Следственные органы также задействуют инструменты для мониторинга и анализа активности в телекоммуникационных сетях. К таким инструментам относятся, в частности, приложения для отслеживания переписки в мессенджерах, мониторинга посещения интернет-ресурсов и анализа сетевого трафика.

Все технические средства, применяемые в рамках следственных мероприятий, должны находиться на балансе соответствующего ведомства или быть официально закреплены за конкретным сотрудником. Однако на практике часто фиксируются следственные действия с использованием личных мобильных устройств следователей, что является незаконным. Организационные сложности не могут служить оправданием для применения личной техники, поскольку это может поставить под сомнение законность полученных доказательств и создать риск их подделки или утечки информации.

В связи с технической сложностью и спецификой следственных мероприятий участие квалифицированного специалиста в области информационных технологий и кибербезопасности становится необходимым. Такой специалист способен обеспечить доступ к конфиденциальной информации, восстановить утраченные цифровые данные, определить местоположение устройств, использованных при

совершении преступления, и решить другие значимые задачи. Отсутствие компетентного технического эксперта может привести к затягиванию процесса расследования или его невозможности.

Перед началом совместного производства тех или иных следственных действий следователь обязан проверить квалификацию специалиста и удостовериться в отсутствии личной заинтересованности последнего в деле. Помимо разъяснения процессуальных прав и обязанностей участников следственных действий, необходимо обратить внимание на соблюдение норм, установленных не только Уголовно-процессуальным кодексом Российской Федерации, но и Федеральным законом «О персональных данных» № 152-ФЗ [1] и Федеральным законом «Об информации, информационных технологиях и о защите информации» № 149-ФЗ [2]. Тесное взаимодействие между следователем и техническим экспертом обеспечивает законность и эффективность следственных действий: следователь отвечает за юридическую сторону, а технический эксперт – за техническую точность и эффективность используемых инструментов.

Таким образом, расследование дистанционных преступлений требует использования современных криминалистических методов и эффективного взаимодействия с цифровыми сервисами. Расследуя дистанционные преступления, совершаемые на интернет-платформах для разменей объявлений, следователь сталкивается с рядом сложностей. Решением данных проблем в первую очередь станет совершенствование российского законодательства, а именно внесение в Уголовно-процессуальный кодекс статей с более подробной регламентацией производства следственных действий в данной области как, например, осмотр сетевых информационных ресурсов, а также возможность осуществления ряда процессуальных действий дистанционно, что позволит снизить возникающие процессуальные ошибки, а также ускорить процесс расследования данного рода преступлений.

Список литературы

1. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_61798/.
3. Статистические данные МВД России [Электронный ресурс] URL: <https://мвд.рф/reports/item/64450541/>.
4. Агеев В. В. Методика расследования компьютерных преступлений. – М.: ЮНИТИ, 2022.
5. Поляков В. В. Основные методики расследования компьютерных преступлений. – Барнаул: издательство алтайского государственного университета, 2024.
6. Иванов И. И. Особенности доказывания по уголовным делам о дистанционном мошенничестве // Уголовное право. – 2023. – № 4. – С. 45–49.

7. Кузнецов А. В., Егорова Т. М. Использование цифровых следов при расследовании преступлений. – СПб.: Изд-во РГУП, 2023.

8. Паутов С. С., Пидусов Е. А. Основные схемы мошенничества, совершаемого с использованием интернет-сервисов размещения объявлений // Вестник Краснодарского университета МВД России, 2023, № 4 (62) [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/osnovnye-shemy-moshennichestva-sovershaemogo-s-ispolzovaniem-internet-servisov-razmescheniya-obyavleniy/viewer>.

9. Семенихина Т. Н. Методика расследования дистанционных мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий под предлогом продажи (покупки) различных товарно-материальных ценностей на интернет-сайтах // Вестник Воронежского института МВД России, 2022. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/metodika-rassledovaniya-distantsionnyh-moshennichestv-sovershaemyh-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy>.

10. Стащенко С. П. К вопросу о классификации прав граждан в информационной сфере / С. П. Стащенко, А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 5. – С. 219–222. – DOI 10.24412/2073-0454-2023-5-219-222. – EDN TUUOVO.

11. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

12. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

13. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

14. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

15. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

16. Константинов А. В. Правовое регулирование интернет вещей (IoT): состояние и риски использования / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2024. – С. 35–37. – EDN HPTYOY.

Малина А. Г.¹,
*курсант института подготовки
сотрудников для органов предварительного
расследования Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Рудин А. В.,
*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК МЕТОД СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

В настоящее время число преступлений, совершенных в киберсреде продолжает расти и наращивает свои темпы. На собрании членов Совета Федерации заявили, что количество киберпреступлений в России за минувшие пять лет выросло в 2,3 раза – с 294 тыс. в 2019 г. до 677 тыс. в 2024 году. При этом за последнее время сам характер киберпреступности заметно изменился: специалисты отмечают рост утечек и незаконной коммерциализации персональных данных, а в 2023 г. к нему добавилась новая угроза – выросло количество кибератак с целью разрушения информационных систем, а не с целью создания инфоповода или получения выкупа.

Отмечается, что социальная инженерия остается одним из основных методов совершения киберпреступлений. При этом раскрываемость подобных дел остается недостаточной – до суда доходит лишь четверть. Люди – социальные существа. Практически в каждого человека с детства закладывают информацию, о том, что необходимо быть честными по отношению друг к другу и подвергать сомнению сказанные вещи другим человеком без уважительной причины – это неправильно. К сожалению, эти социальные тонкости могут превратить нас в самое слабое звено в системе информационной безопасности. Слишком часто взломы возникают не из-за технических недостатков, а из-за того, что люди, позволяя киберпреступникам себя в чем-то убедить и тем самым ослабить бдительность и собственную охрану [1]. Именно такое воздействие на людей в науке получило название «социальная инженерия».

С. С. Созаев и Д. А. Кунашев определяют социальную инженерию как искусный метод управления психологией человека без использования технических приемов, взломов для получения персональной информации, доступа к чему-либо конфиденциальному [2]. В. В. Суворова и Л. А. Суворова дают более развернутое и конкретизированное определение социальной инженерии, включая

¹ © Малина А. Г., 2025.

уголовно-правовые и криминалистические составляющие: вид совершения компьютерных преступлений, направленный на несанкционированное получение информации путем использования слабых мест в психике человека, к которым относится инициативность, нервно-психическая слабость, чувствительность [3].

Таким образом, можно сказать, что социальная инженерия – это метод, используемый киберпреступниками для манипулирования людьми с целью получения доступа к конфиденциальной информации для совершения киберпреступлений. Необходимо заметить, что законодательного закрепления данного требования не существует, мы обнаруживаем пробел в данной области, так как единое понимание привело бы к более точному пониманию и остальных процессов, связанных с киберпреступностью.

Рассмотрев понятие социальной инженерии, возникает вопрос: почему именно с ее помощью так часто происходят киберпреступления? Как обезопасить себя от данного метода совершения киберпреступлений? Поиск ответов на данные вопросы стал очень популярен и востребован в 21 в. Большинство людей старше 55-60 лет не умеют в полной мере пользоваться мобильными приложениями в своих смартфонах. При этом стоит отметить, что жертвами киберпреступлений зачастую становятся и молодые люди. В какой-то степени можно сказать, что возраст не имеет значения, а важным фактом является образованность человека, умение не вестись на манипуляции других людей, обладание критическим мышлением и некоторые другие факты. Необходимо обучать своих детей и старших в семье, как правильно пользоваться гаджетом, по каким ссылкам не стоит переходить и какие коды не нужно диктовать посторонним людям. Такая профилактика внутри семьи может иметь фундаментальное значение для выстраивания безопасного пользования интернетом.

Также необходимо отметить, что в связи с активными мошенническими и хакерскими действиями операторы сотовой связи и госучреждения вводят дополнительные меры профилактики и борьбы с киберпреступлениями. Так, у оператора сотовой связи «МТС» за дополнительную плату можно приобрести такую функцию, как защитник от спам-звонков. Это очень упрощает пользование гаджетом, всегда можно увидеть кто тебе звонил и с какой целью. Технологии беспрерывно продолжают развиваться. И виды мошеннических действий все также продолжают приобретать новые краски. В связи с этим для граждан Российской Федерации появилась новая возможность, такая как самозапрет на выдачу кредитов. Мошенники с использованием информационных технологий все чаще стали оформлять кредиты на граждан без их ведома, поэтому такая мера поможет защитить людям свои денежные средства.

Анализируя все вышеперечисленное, мы делаем вывод, что с развитием киберпреступности непрерывно развиваются и меры по их противодействию.

Чтобы мы могли противодействовать киберпреступлениям с использованием социальной инженерии, необходимо знать их техники:

1. Фишинг (электронной почты, текстовых сообщений, «подводная охота»). Является наиболее популярным способом социальной инженерии. Задачей фишинга электронной почты является отправка большому количеству человек спам-сообщений на адрес электронной почты так, чтобы сообщение выглядело,

как будто оно было отправлено компанией или организацией, которой человек доверяет. Подобные электронные письма легко создавать в настоящее время, используя готовые фишинговые наборы, которые содержат предварительно разработанные шаблоны электронных почт, известных компаний. В спам-письме содержится ссылка на фишинговый сайт, предназначенный для сбора имен пользователей и паролей [4].

2. Не менее популярный способ социальной инженерии – претекстинг. Это заранее грамотно написанный сценарий действий преступника, результатом которого является в 80 % случаев полученная от потерпевшего информация, необходимая киберпреступнику. Данный способ осуществим при помощи телефонного звонка [5].

3. «Троянский конь» – вид вредоносной программы. Компьютерные трояны содержат в себе разрушительную нагрузку. Вложения электронной почты, содержащие скрытые вредоносные программы, являются формой трояна. Хитрость социальной инженерии заключается в том, что электронная почта, с которой отправляется вредоносный файл, исходит от надежного отправителя (коллега, друг, член семьи или компании, с которой вы ведете бизнес) [6].

4. Вишинг (голосовая запись). Данный способ осуществляется путем телефонного звонка, с помощью которого, например, у клиентов банков выводится конфиденциальная информация. Главной особенностью данного способа является заранее подготовленные голосовые сообщения от якобы специалистов данной компании (например, Сбербанка) [7].

Мы рассмотрели основные техники совершения киберпреступлений с использованием инженерии. Можно заметить, что данные методы очень разнообразны и многогранны. Необходимо всегда следить за состоянием киберпреступности и знать способы противодействия ей.

Таким образом, можно сделать вывод, что киберпреступность с использованием социальной инженерии в последнее время считается преимущественным видом преступной деятельности, и мы можем спрогнозировать, что в ближайшее десятилетие данная тенденция будет сохраняться. Чтобы обезопасить себя и своих близких, предпринимайте меры для безопасного использования интернет-ресурсов.

Список литературы

1. Янгаева М. О. Методы (техники) социальной инженерии, используемые при совершении преступлений в сфере компьютерной информации // Криминалистика: вчера, сегодня, завтра. – 2021. – Т. 18. – № 2. – С. 145–151.
2. Созаев С. С. Социальная инженерия, ее техники и методы ее противодействия / С. С. Созаев, Д. А. Кунашев // Вестник науки : международный журнал. – 2020. – № 2 (23). – Т. 1. – С. 85–88.
3. Суворова В. В. Совершение преступлений с использованием социальной инженерии: постановка проблемы / В. В. Суворова, Л. А. Суворова // Теория и

практика приоритетных научных исследований: сборник научных трудов по материалам VIII Международной научно-практической конференции. – Изд. МНИЦ «Наукосфера», 2019. – С. 71–74.

4. Кузнецов М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Сим-дянов. – СПб.: БХВ-Петербург. – 2007. – 368 с.

5. Митник К. Д. Искусство обмана / К. Д. Митник, В. Д. Саймон // Компания АйТи. – 2004. – 360 с.

6. Ревенков П. В. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания / П. В. Ревенков, А. А. Бердюгин // Национальные интересы: приоритеты и безопасность. – 2017. – № 9 (354). – С. 1747–1760.

7. Созаев, С.С. Социальная инженерия, ее техники и методы ее противодействия / С.С. Созаев, Д.А. Кунашев // Вестник науки : международный журнал. - 2020. - № 2(23). -Т. 1. - С. 85-88.

8. Стащенко С. П. К вопросу о классификации прав граждан в информационной сфере / С. П. Стащенко, А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 5. – С. 219–222. – DOI 10.24412/2073-0454-2023-5-219-222. – EDN TUUOVO.

9. Константинов А. В. Перспективы развития и использования искусственного интеллекта в целях противодействия преступлениям в сфере информационно-телекоммуникационных технологий / А. В. Константинов // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов, Москва, 30 марта 2023 года / сост. А. В. Константинов. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 80–82.

10. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.

11. Информационное право : учебное пособие / В. В. Пушкарёв, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.

12. Пушкарёв В. В. Информационное право : терминологический словарь / В. В. Пушкарёв, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.

13. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарёв, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.

14. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.

Мальцева В. А.¹,
курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Тололов А. В.,
доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОКАЗАНИЯ МЕДИЦИНСКОЙ ПОМОЩИ С ПРИМЕНЕНИЕМ ТЕЛЕМЕДИЦИНСКИХ ТЕХНОЛОГИЙ

В 21 веке ученые достигли огромных успехов во всех сферах жизни общества, будь то образование или правоохранительная деятельность. Время, в которое мы живем можно назвать «информационной эрой». Сферу здравоохранения различные новшества так же не обошли стороной. Появилось множество новейшей техники, а также различных специфических технологий. Постепенно врачи начинают отходить от применения бумажных носителей, так, например, в поликлиниках появилась возможность записываться на прием к врачу путем использования интернет-сети через приложение «ЕМИАС».

Гражданам стало куда проще посещать врачей, ведь дистанционно можно выбрать удобное время и дату для посещения специалиста. Появилась тенденция ведения электронных карт пациента, которая позволяет разгрузить сотрудников медицинских организаций от рутинной работы и обеспечить более удобное хранение информации. Также стоит упомянуть о появлении специальных приложений (Symptomate, Ada и т. д.), в которых используется искусственный интеллект для помощи гражданам в диагностировании заболеваний путем консультаций, анкетирования и аналитики информации о симптомах, поиске специалиста определенной отрасли. Эти приложения относятся к новейшей отрасли здравоохранения – телемедицине.

Телемедицина – это сфера дистанционных медицинских услуг, которая несет в себе возможность получения медицинских консультаций удаленно, с использованием информационно-телекоммуникационных технологий. Такое новшество позволяет гражданам своевременно получать медицинскую помощь. Основную популярность телемедицина начала набирать в период пандемии «Covid-19», поскольку именно в то время была актуальна дистанционная медицинская помощь, так как люди не могли выходить из дома. Но несмотря на окончание

¹ © Мальцева В. А., 2025.

пандемии, актуальность этой сферы продолжает расти, такой рост объясняется удобством данной технологии, например, человек, болеющий серьезным заболеванием имеет возможность получить консультацию специалиста на расстоянии, не выходя из дома.

Рассматриваемая деятельность с точки зрения права регулируется: Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; приказом Минздрава России от 30.11.2017 № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий». В соответствии с приказом Минздрава России № 965н, помощь гражданам с использованием телемедицинских технологий осуществляется исключительно квалифицированными специалистами из числа организаций, внесенных в единую государственную информационную систему. Оказывать медицинские консультационные услуги дистанционно могут организации любой формы собственности, т. е. частные клиники, государственные и муниципальные учреждения.

Оказание медицинских услуг с применением телемедицинских технологий в России осуществляется в соответствии с общими лицензионными требованиями, предъявляемыми к медицинской деятельности в целом. При этом, как отмечают специалисты, такие требования специальным образом не адаптированы под телемедицину [1], в связи с чем представляется целесообразным внести изменения в правила лицензирования медицинской деятельности по оказанию медицинских услуг с применением телемедицинских технологий.

Важным аспектом телемедицинской деятельности является вопрос об ответственности лиц, оказывающих такие услуги. В соответствии с указанным федеральным законом, такая деятельность осуществляется соотносительно стандартам медицинской помощи, то есть ответственность предусматривается наравне с обычной – традиционной медицинской помощью.

Необходимо рассмотреть проблему того, что несмотря на существование телемедицинских технологий, пациентам необходимо учитывать тот факт, что для применения дистанционных медицинских консультаций больному необходимо явиться на прием к врачу очно. Что означает, что невзирая на то, что телемедицина растет и набирает популярность, будучи удобной для общества, к полному переходу на использование таких технологий в данный период времени невозможно. Невозможность перехода к полноценному лечению пациентов с использованием телемедицинских технологий, обосновывается определенными факторами: социальным, технологическим и экономическим [2].

Социальный фактор основывается на том, что многие люди при решении вопроса о своем лечении, предпочитают взаимодействие в реальном времени, т. е. общение непосредственно с медицинским специалистом, также стоит сказать, что существует часть общества, которая не имеет доверия к технологическим новшествам и нововведенным сферам деятельности. Технологический фактор означает, что с ростом цифровизации так же растет и потребность в новой технике. Такую потребность зачастую не удается реализовать из-за недостаточности специалистов в новых, специфических областях, а также недостаточности знаний в них. Воплощение технологических новшеств требует большого количества

времени, что не позволяет их реализацию в короткий срок. Экономический фактор отмечает то, что создание информационно – телекоммуникационных технологий в телемедицине требует затраты больших средств, что так же является барьером к их скорому развитию.

Цифровизация является неотъемлемой частью развития любой сферы в настоящее время. Безусловно, положительно следует оценивать процессы цифровизации в области здравоохранения. Вместе с тем важно своевременно совершенствовать правовое регулирование указанных общественных отношений, обеспечивая баланс между соблюдением прав граждан, охраной их жизни и здоровья, с одной стороны, и реализацией задач по развитию информационного общества в РФ – с другой.

Список литературы

1. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ (последняя редакция) // СПС «КонсультантПлюс».
2. Приказ Минздрава России от 30.11.2017 № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий» / Зарегистрирован в Минюсте России 09.01.2018 № 49577.
3. Журавлёв М. С., Тягай Е. Д. Правовые проблемы телемедицины. Киберфизические системы, имплантированные в организм человека // Доклад НИУ ВШЭ. 2021. С. 5.
4. Шадеркин И. А. Барьеры телемедицины и пути их преодоления // Российский журнал телемедицины и электронного здравоохранения выпуск № 2. 2022. С. 59–76.
5. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 263 с. – ISBN 978-5-4497-4085-4. – EDN FGPMCO.
6. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. – Москва : Ай Пи Ар Медиа, 2025. – 197 с. – ISBN 978-5-4497-4146-2. – EDN UICMXX.
7. Пушкарев В. В. Информационное право : терминологический словарь / В. В. Пушкарев, А. В. Константинов. – Москва : Ай Пи Ар Медиа, 2025. – 167 с. – ISBN 978-5-4497-4056-4. – EDN TGFRRN.
8. Право в сфере информационных технологий : практикум для СПО / В. В. Пушкарев, А. В. Константинов, С. П. Стащенко [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2025. – 62 с. – ISBN 978-5-4497-3726-7. – EDN FJISXZ.
9. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

10. Пушкарёв В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарёв, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88-92.

Маренкова С. В.¹,
курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета МВД России
имени В.Я. Кикотя

Научный руководитель:
Поликарпова Е. В.,
старший преподаватель
кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя

КОММЕРЧЕСКАЯ ТАЙНА КАК ВИД КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Коммерческая тайна играет важную роль в обеспечении устойчивости и конкурентоспособности хозяйствующего субъекта. Под этим понятием принято понимать информацию, которая не подлежит свободному распространению и используется в предпринимательской деятельности для получения выгоды, улучшения рыночных позиций или укрепления репутации компании [4, с. 33–36].

Для отнесения определенных сведений к коммерческой тайне, необходимо соблюдение ряда условий. Прежде всего, такая информация должна быть:

- связана с осуществлением предпринимательской или производственной деятельности;
- обладать коммерческой ценностью вследствие неосведомленности третьих лиц;
- защищена от свободного доступа со стороны неуполномоченных к пользованию лиц;
- оформлена в соответствии с внутренними актами организации;
- исключать в составе наличия государственной тайны.

На практике к сведениям, причисленным к коммерческой тайне, относят данные о технологиях, производственных рецептах, финансовых планах, стратегии развития, результатах внутреннего анализа, клиентских базах и других аспектах, знание которых способно повлиять на конкурентную среду.

Законодательство Российской Федерации регулирует порядок обращения с такого рода информацией через положения Гражданского кодекса, а также специализированный Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

Согласно ст. 3, указанного закона, статус коммерческой тайны может быть присвоен любой информации, если она:

¹ © Маренкова С. В., 2025.

1. Прямо связана с ведением бизнеса.
2. Не подлежит разглашению в силу прямых норм иных законов (например, гостайна).
3. Принадлежит конкретному юридическому лицу или индивидуальному предпринимателю.
4. Имеет потенциальную ценность для конкурентов или других заинтересованных лиц.
5. Является предметом мер по ограничению доступа и обеспечению сохранности.

Следует учитывать, что понятие конфиденциальной информации более широкое и включает в себя не только сведения экономического характера, но и иные данные, доступ к которым ограничен по закону или соглашению. Коммерческая тайна же – это узкоспециализированная категория конфиденциальных сведений, обладающая самостоятельным правовым режимом.

Федеральный закон № 98-ФЗ четко устанавливает перечень информации, которой запрещено придавать статус коммерческой тайны. В частности, к ней не могут относиться [8, с.3–4]:

- учредительные документы юридических лиц;
- сведения, подлежащие включению в государственные реестры;
- информация о состоянии окружающей среды, санитарной и пожарной безопасности;
- данные о численности персонала, уровне оплаты труда, социальных выплатах и нарушениях закона;
- сведения о задолженностях по заработной плате;
- данные о государственных закупках, конкурсах, аукционах;
- финансовые показатели некоммерческих организаций;
- обязательные к раскрытию сведения согласно другим федеральным законам.

Разглашение или незаконное использование сведений, охраняемых в рамках коммерческой тайны, может повлечь за собой различные виды юридической ответственности: дисциплинарную, административную и уголовную.

Уголовный кодекс Российской Федерации (ст. 183) предусматривает наказания за неправомерное получение и распространение коммерческой тайны. После изменений, внесенных Федеральным законом № 193-ФЗ от 29 июня 2015 г., максимальные штрафы были существенно увеличены:

- до 500 000 рублей по части 1 статьи;
- до 1 миллиона рублей по части 2;
- до 1,5 миллиона рублей по части 3.

Характерным примером служит дело, в котором организация пыталась привлечь к ответственности бывшего сотрудника за использование клиентской базы. Компания ссылаясь на то, что сотрудник после увольнения начал аналогичный бизнес и стал работать с теми же клиентами.

Однако суд установил, что несмотря на наличие в трудовом договоре пункта о неразглашении информации, компания не оформила надлежащим образом режим коммерческой тайны в отношении этих сведений. Не были приняты необходимые внутренние документы, не оформлялись ограничения доступа, не велся учет лиц, имевших к базе доступ. В результате иск остался без удовлетворения – клиентская база не была признана охраняемой.

Таким образом, для надлежащей защиты коммерческой тайны требуется не только правовая декларация соответствующего режима, но и его фактическое внедрение в организационную структуру. Необходима системная работа по ограничению доступа, фиксации прав пользователей, заключению соглашений и ведению внутреннего документооборота. Только при соблюдении этих условий организация может рассчитывать на эффективную правовую защиту своих экономически значимых сведений.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Доступ из СПС «КонсультантПлюс» (дата обращения: 12.05.2025).
2. Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ (с изм. и доп.) – [Электронный ресурс] СПС «Консультант плюс» 2024.
3. Афанасьева В. И., Шагиева Р. В., Вармунд В. В. Коммерческое право. Учебник для магистратуры. М.: КноРус, 2020. – 278 с.
4. Вершинина Е. С., Щербакова М. П. Коммерческая тайна: понятие, условия обработки // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. №1 (57). – С. 33–36. – URL: <https://cyberleninka.ru/article/n/kommercheskaya-tayna-ponyatie-usloviya-obrabotki> (дата обращения: 12.05.2025).
5. Напалкова Д. В. Коммерческая тайна в цифровую эпоху. Правовой механизм обеспечения защиты коммерческой информации / Д. В. Напалкова. – Текст: непосредственный // Молодой ученый. – 2023. – № 13 (460). – С. 263–266. – URL: <https://moluch.ru/archive/460/101234/> (дата обращения: 12.05.2025).
6. Северин В. А. Коммерческая тайна в России: моногр. / В. А. Северин. – М.: Зерцало, 2015. – 977 с.
7. Определение Первого кассационного суда общей юрисдикции от 05.06.2023 по делу № 88-18752/2023.
8. Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ (с изм. и доп.) – [Электронный ресурс] СПС «КонсультантПлюс» 2025.
9. Пушкарев В. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют / В. В. Пушкарев, А. В. Токолов // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
10. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Наянзин Н. В.¹,
студент 4 курса, факультет права
НИУ «Высшая школа экономики»

Ошманкевич Е. Р.²,
студент 4 курса, факультет права
НИУ «Высшая школа экономики»

Научный руководитель:
Пушкарёв В. В.,
доцент департамента уголовного права,
процесса и криминалистики
НИУ «Высшая школа экономики»,
кандидат юридических наук, доцент

ПРИМЕНЕНИЕ ПРОЦЕДУР KYC/AML В ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ НА КРИПТОВАЛЮТНЫХ БИРЖАХ: ОПЫТ ЮЖНОЙ КОРЕИ

Южная Корея занимает лидирующие позиции на мировом рынке криптовалют как одна из стран с одним из самых динамично развивающихся криптовалютных секторов [1]. Глобальная активизация цифровых активов и интенсивное развитие криптобирж требуют от государства разработки и внедрения механизмов, способных обеспечить прозрачность сделок, защиту прав инвесторов и противодействие преступной деятельности. В этом контексте особое значение приобретают процедуры KYC (Know Your Customer – «Знай своего клиента») и меры AML (Anti-Money Laundering – противодействие отмыванию денег). Данные механизмы стали неотъемлемой частью государственного регулирования деятельности криптовалютных бирж, позволяя выявлять и пресекать попытки легализации денежных средств, полученных преступным путем [2, с. 130]. Южнокорейский опыт демонстрирует, каким образом комплекс мер, направленных на обязательную идентификацию клиентов и контроль за финансовыми операциями, может снизить риски использования платформ для финансирования преступной деятельности.

Процедуры KYC представляют собой набор мер, направленных на установление и проверку личности клиента [10, с. 43]. Они включают в себя обязательное предоставление документов, подтверждающих личность, а также проведение внутреннего контроля криптовалютной биржей. В свою очередь, меры AML нацелены на выявление и пресечение операций, связанных с отмыванием денег и финансированием терроризма [11]. Ключевыми аспектами являются мониторинг подозрительных транзакций, сбор и анализ финансовых данных, а также взаимодействие с банковскими и правоохранительными органами. В условиях

¹ © Наянзин Н. В., 2025.

² © Ошманкевич Е. Р., 2025.

быстрого развития цифровых технологий и расширения сферы криптовалют такие меры становятся особенно актуальными для защиты как инвесторов, так и финансовой стабильности государства.

С сентября 2021 г. власти Южной Кореи ввели обязательную регистрацию всех криптовалютных бирж, действующих на территории страны [6]. Для получения лицензии биржи должны не только налаживать партнерские отношения с местными банками, но и внедрять строгие процедуры идентификации клиентов (KYC). В рамках данной практики биржи обязаны проверять подлинность личных данных пользователей, что позволяет исключить возможность анонимной торговли и повышает прозрачность финансовых операций. Федеральные органы акцентируют внимание на необходимости проведения комплексных проверок всех участников криптовалютного рынка, что способствует снижению потенциальных рисков.

Одна из основных задач введенных регулятивных мер – предотвращение использования криптовалютных бирж в целях отмывания денег. Регуляторы Южной Кореи обязали криптовалютные компании передавать банкам информацию о подозрительных операциях и не допускать смешивания активов пользователей с собственными средствами бирж [4]. Такие меры предусматриваются как обязательная часть требований для получения лицензии и дальнейшего функционирования платформ на территории страны. Контроль за выполнением мер AML осуществляется с помощью регулярных проверок, проводимых как саморегулируемыми организациями, так и государственными органами, что позволяет оперативно реагировать на случаи мошеннических операций [8].

Ключевыми органами, осуществляющими контроль и надзор за соблюдением процедур KYC/AML, являются Комиссия по финансовым услугам (FSC) и Финансовая служба надзора (FSS) [3]. FSC в качестве главного регулятора определяет требования к криптовалютным биржам, включая обязательную проверку личности пользователей и проведение мер по борьбе с отмыванием денег. FSC также имеет полномочия по проведению проверок, наложению штрафных санкций, а в случае выявления систематических нарушений – приостановлению или отзыву лицензии платформы. FSS, действуя совместно с FSC, проводит оперативный мониторинг деятельности криптобирж, следит за соблюдением мер KYC/AML и взаимодействует с правоохранительными органами при расследовании преступлений, связанных с цифровыми активами.

Южнокорейская модель регулирования основывается на ряде последовательных реформ, направленных на обеспечение безопасности операций на криптобиржах [7]. В рамках новейшего законодательства вводятся следующие меры: во-первых, криптовалютные биржи регистрируются для осуществления деятельности в Республике Кореи в качестве операторов виртуальных активов и подчиняются строгим стандартам, предусматривающим обязательное проведение процедур идентификации клиентов. Для повышения прозрачности всех операций введен запрет на использование анонимных аккаунтов. Все пользователи криптовалютных платформ обязаны пройти верификацию личности, что позволяет снизить уровень преступной активности. Кроме того, криптобиржи обязаны

обеспечивать систему мониторинга операций, которая позволяет выявлять транзакции, потенциально связанные с отмыванием денег, и передавать данные в соответствующие финансовые и правоохранительные органы [7]. Правительственные органы, в том числе FSC и FSS, регулярно проводят проверки криптовалютных бирж, отслеживают выполнение предписанных мер и применяют санкции в случае выявления нарушений.

Несмотря на развитое правовое регулирование, практика применения процедур KYC/AML сталкивается с рядом проблем и ограничений. Прежде всего, существуют сложности с эффективной идентификацией пользователей. Даже при обязательном проведении процедур верификации остается вероятность использования поддельных документов или обхода системы проверки [5, с. 1]. Кроме того, смешанное хранение криптоактивов пользователей с активами биржи создает дополнительные риски: в случае банкротства платформы средства пользователей могут быть подвергнуты изъятию кредиторами.

Законодательные меры, направленные на борьбу с отмыванием денег, были адаптированы для соответствия международным стандартам, в частности рекомендациям FATF [9, с. 143]. Однако критика также касается чрезмерного регулирования, которое, с одной стороны, должно защищать рынок от преступной деятельности, а с другой – не создавать излишних барьеров для функционирования инновационных технологий.

Важным вопросом остается и эффективность мониторинга трансграничных операций, где недостаточная интеграция внутренних систем контроля с международными механизмами может снижать потенциал обнаружения и пресечения подозрительных операций.

Таким образом, эволюция законодательства Южной Кореи демонстрирует последовательный переход от ограничительных мер к формированию комплексной системы контроля за деятельностью криптовалютных бирж. Применение процедур KYC и мер AML становится важным инструментом в борьбе с преступлениями, связанными с цифровыми активами. Обязательная регистрация бирж, запрет анонимной торговли и интеграция с банковским сектором позволяют обеспечить прозрачность операций и минимизировать риски использования платформ для отмывания денег. При этом остаются актуальными вопросы совершенствования системы верификации и повышения эффективности надзора за трансграничными операциями. Южнокорейский опыт демонстрирует, что последовательное и гибкое совершенствование нормативной базы является залогом стабильного развития криптовалютного сектора и защиты финансовых интересов государства и его граждан.

Список литературы

1. Вона обогнала доллар по объемам торгов на криптовалютных биржах [Электронный ресурс] // Сайт РБК.Крипто. URL: <https://www.rbc.ru/crypto/news/661e8d239a7947d540a1277d> (дата обращения: 10.04.2025).

2. Долгиева М. М. Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. 2019. № 4.

3. Закон о защите пользователей виртуальных активов (가상자산 이용자 보호 등에 관한 법률 (약칭: 가상자산이용자보호법) [시행 2024. 7. 19.] [법률 제 20372 호, 2024. 3. 12., 타법개정]).

4. Исследование общеправительственного и законодательного контроля над криптовалютной преступностью – с фокусом на поправках к Закону о финансовой разведке (정제용. 암호화폐 범죄 관련 범정부적 및 입법적 통제에 대한 연구-특정금융정보법 개정안을 중심으로 //경찰학연구). – 2021. – Т. 21. – №. 1. – С. 80

5. Криптовалюты и государство: на примере Южной Кореи (Ahn C., Obermeier N. Cryptocurrency and the State: Evidence from South Korea). – 2024.

6. [Пресс-релиз] Постановление о введении в действие «Закона о защите пользователей виртуальных активов» [Электронный ресурс] // FSC. URL: <https://www.fsc.go.kr/no010101/81214?srchCtgry=&curPage=31&srchKey=&srchText=&srchBeginDt=&srchEndDt=https%2F%2Fdecrypt.co%2F60915%2Fsouth-korea-cracks-down-crypto-money-laundering> (дата обращения: 10.04.2025).

7. [Пресс-релиз] Специальные меры по искоренению спекуляций виртуальной валютой (가상통화 투기근절을 위한 특별대책) [Электронный ресурс] // Официальный сайт FSC. URL: <https://www.fsc.go.kr/no010103/24649?srchCtgry=&curPage=12&srchKey=&srchText=&srchBeginDt=&srchEndDt=> (дата обращения: 10.04.2025).

8. Предложение DAXA по саморегулированию (DAXA 자율규제안) [Электронный ресурс] // Digital Asset Exchange Alliance. URL: <https://kdaxa.org/support/regulation.php> (Дата обращения: 10.04.2025).

9. Сравнительное исследование регулирования виртуальной валюты (백승윤 et al. 가상화폐 규제에 관한 비교법적 고찰 //법학연구). – 2021. – Т. 21. – №. 3. – С. 143.

10. Фазилов Ф. М. Роль и значение системы «KYC» в предупреждении отмывания денег // Universum: экономика и юриспруденция. 2021. № 7 (82).

11. Financial Action Task Force. Virtual Currencies: Key Definitions and Potential AML/CFT Risks. 2014 // URL: <http://fatf-gafi.org/topics/methodsandtrends/documents/virtual-currencydefinitions-aml-cft-risk.html> (дата обращения: 10.04.2025).

12. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарёв, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

13. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Руденко М. М.¹,
курсант института психологии
служебной деятельности ОВД
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Соломатина Е. А.,
доцент кафедры криминологии
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

К ВОПРОСУ О ПРОФИЛАКТИКЕ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В ТЕРРОРИСТИЧЕСКУЮ ДЕЯТЕЛЬНОСТЬ С ПОМОЩЬЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

С появлением информационных технологий в нашем обществе значительно снизился уровень сложности в процессе поиска информации. А как известно, информация в сети интернет, так называемого «фильтра» не содержит, что в свою очередь создает своего рода негативные последствия и проблемы.

Самыми активными пользователями Интернет-пространства являются несовершеннолетние. В 2023 г. было проведено исследование, в ходе которого было выявлено, что 99 % подростков имеют хотя бы один профиль в социальной сети. А сегодня остро стоит вопрос профилактики вовлечения несовершеннолетних в террористическую деятельность с помощью информационных технологий.

По данным Федеральной службы безопасности России в список террористических организаций включены 61 организация, а для осуществления своей идеологической, террористической деятельности им очень нужны так называемые «чужие руки». Вот именно несовершеннолетние очень подходят для таких целей.

Как отмечал писатель Джон Хорган в своих книгах (профессор факультета психологии, где он руководит группой по изучению насильственного экстремизма) – «Терроризм – есть стратегия, тактика которого – насилие».

Исходя из определения, закрепленного в ст. 3 Федерального закона № 35-ФЗ «О противодействии терроризму» террористическая деятельность подразумевает под собой следующее:

1. Организацию, планирование, подготовку, финансирование и реализацию террористического акта.
2. Подстрекательство к террористическому акту.
3. Организацию незаконного вооруженного формирования, преступного сообщества, организованной группы для реализации террористического акта, а равно участие в такой структуре.
4. Вербовку, вооружение, обучение и использование террористов.

¹ © Руденко М. М., 2025.

5. Информационное или иное пособничество в планировании, подготовке или реализации террористического акта.

6. Пропаганду идей терроризма, распространение материалов или информации и т. п. [3].

Информационно-телекоммуникационные технологии являются главным инструментом террористов по следующим причинам:

1. Предоставляется возможность активной пропаганды той или иной идеологии.

2. Предоставляется возможность создавать сообщества (сети сообществ), где те или иные взгляды подкрепляются различными фактами и обсуждаются с несовершеннолетним.

3. Предоставляется возможность дистанционно обучать несовершеннолетних методам террористической деятельности [2].

Отметим, что главными психологическими особенностями несовершеннолетних являются следующие аспекты:

1. Эмоциональные колебания, подразумевающие под собой резкие скачки в поведении и настроении.

2. Состояние нестабильности, ввиду этого мы можем замечать за несовершеннолетними их стремление подражать каким-либо «авторитетам» (как отрицательным, так и положительным) и подверженность определенным субкультурам.

3. Эмоциональная уязвимость, зачастую проявляющаяся в чрезмерной наивности.

4. Стремление к самореализации и к самовыражению, желание выделиться. [1].

Все это перечисленное и многое другое делает несовершеннолетнего потенциальной мишенью для злоумышленника.

Думается, что меры профилактики по вовлечению несовершеннолетних в террористическую деятельность путем использования информационно-телекоммуникационных технологий должны включать:

1. Создание специальных программ, которые будут иметь своей целью повышения правовой, а также цифровой грамотности несовершеннолетних.

2. Проведение профилактических занятий в образовательных организациях на такие темы, как: механизмы манипуляций, безопасное «чистое» поведение в социальных сетях, объяснение детям куда обращаться при попытке вовлечения или воздействия на них со стороны злоумышленников.

3. От семьи требуется систематическое участие в жизни своих детей, а также беседы на тему безопасности в интернете, располагать детей к открытому общению, объяснение несовершеннолетним как себя вести в той или иной ситуации (в частности, при попытке воздействия на них).

4. Проведение сотрудниками подразделений по делам несовершеннолетних, в том числе и оперативными сотрудниками центров противодействия экстремизму профилактических бесед по темам, касающимся вовлечения несовершеннолетних в террористическую, экстремистскую деятельность через Интернет-пространство.

Таким образом, профилактика вовлечения несовершеннолетних в террористическую деятельность является сложной и многогранной задачей, требующей совместной работы от всех субъектов предупредительной деятельности, что позволит значительно снизить риски вовлечения несовершеннолетних в террористическую деятельность.

Список литературы

1. Кирьянова С. П. Причины вовлечения несовершеннолетних в террористическую деятельность / С. П. Кирьянова, И. К. Воронин // Проблемы и перспективы юридической науки и практики: трибуна молодых: Материалы межвузовской молодежной научно-практической конференции, Хабаровск-Южно-Сахалинск, 15–16 ноября 2024 года. – С. 92–97.
2. Соломатникова Д. П. Причины и условия вовлечения несовершеннолетних в экстремистскую и террористическую деятельность / Д. П. Соломатникова // Детство – территория безопасности: Студенческий сборник материалов конференции, Москва, 17–18 ноября 2022 года. – Москва: Издательство «Саратовский источник», 2022. – С. 256–259.
3. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 28.02.2025) «О противодействии терроризму». Информационный ресурс Интернет, сайт <https://www.garant.ru/products/ipo/prime/doc/406740607/> (дата обращения: 05.03.2025).
4. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.
5. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Тамбовцева М. А.¹,

курсант института подготовки сотрудников

для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Поликарпова Е. В.,

старший преподаватель

кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя

ЗАЩИТА КОРПОРАТИВНЫХ ДАННЫХ ОТ УТЕЧЕК И ВЗЛОМОВ

В настоящее время, в современном цифровом мире, где данные стали ценнейшим активом, защита корпоративной информации от утечек и взломов – это не просто желательная мера, а жизненная необходимость. Ведь утечка данных может привести к серьезным финансовым потерям, репутационному ущербу, юридическим последствиям [3, с. 40–45].

Однако, как показывает практика, можно представить, что конфиденциальная информация о ваших клиентах, финансовые отчеты, коммерческие тайны, планы развития – все это попадает в руки злоумышленников. Последствия могут быть катастрофическими.

Тем не менее причин может быть множество, выделим некоторые из них:

1. Слабые пароли и небрежное отношение к безопасности. Чаще всего легко угадываемые пароли, использование одного и того же пароля для разных сервисов, отсутствие двухфакторной аутентификации – все это открывает двери для злоумышленников.

2. Фишинговые атаки. В свою очередь мошенники, выдавая себя за надежных отправителей, выманивают у сотрудников логины, пароли и другую конфиденциальную информацию.

3. Вредоносное программное обеспечение. Как правило, различные вирусы, трояны и другие вредоносные программы могут проникнуть в систему через зараженные файлы, электронные письма или уязвимости в программном обеспечении.

4. Инсайдерские угрозы: Недобросовестные сотрудники, имеющие доступ к конфиденциальной информации, могут намеренно или случайно ее скомпрометировать.

5. Устаревшее программное обеспечение. В совокупности не обновленные системы содержат уязвимости, которые могут быть использованы злоумышленниками.

Тем не менее на практике возникает вопрос, как защитить свои данные?

¹ © Тамбовцева М. А., 2025.

Защита корпоративных данных – это комплексный процесс, требующий постоянного внимания и инвестиций. Вот несколько ключевых шагов:

1. Разработать и внедрить в официальную политику безопасности. Необходимо определить правила и процедуры для защиты данных, включая требования к паролям, правила использования электронной почты и интернета, а также порядок действий в случае инцидента безопасности.

2. Обучить сотрудников. В основном имеет важность регулярного проведения обучения сотрудников по вопросам информационной безопасности, чтобы они знали, как распознавать фишинговые атаки, как создавать надежные пароли и как безопасно использовать корпоративные ресурсы.

3. Использовать надежные пароли и двухфакторную аутентификацию. Однако, необходимо требовать от сотрудников использовать сложные пароли и включить двухфакторную аутентификацию для всех важных учетных записей.

4. Установить и регулярно обновлять антивирусное программное обеспечение. В первую очередь важно защитить свои компьютеры и серверы от вредоносного программного обеспечения.

5. Регулярно создавать резервные копии данных и храните их в безопасном месте.

6. Контролировать доступ к данным. В первую очередь нужно ограничивать доступ к конфиденциальной информации только для тех сотрудников, которым она необходима для выполнения своих обязанностей.

7. Мониторить сетевой трафик. Здесь следует отслеживать сетевой трафик на предмет подозрительной активности.

8. Регулярно проводить аудиты безопасности, чтобы выявить уязвимости и слабые места системе защиты [4, с. 76–80].

Помимо технических мер, в первую очередь не стоит забывать и о юридической составляющей защиты данных. В том числе, необходимо разработать и внедрить юридически грамотные документы, регламентирующие обработку персональных данных, соглашения о неразглашении (NDA) с сотрудниками и партнерами, а также политику конфиденциальности для клиентов. Эти документы должны соответствовать действующему законодательству, например, GDPR (General Data Protection Regulation) в Европе или Федеральному закону №152-ФЗ «О персональных данных» в России.

На рынке представлено огромное количество инструментов и технологий для защиты данных. Выбор конкретных решений зависит от размера компании, ее специфики и бюджета. Вот лишь некоторые примеры:

1. Системы обнаружения и предотвращения вторжений (IDS/IPS). Эти системы анализируют сетевой трафик и выявляют подозрительную активность, блокируя потенциальные атаки.

2. Межсетевые экраны (Firewalls). Они контролируют входящий и исходящий сетевой трафик, блокируя несанкционированный доступ к сети.

3. Системы управления идентификацией и доступом (IAM) позволяют контролировать доступ пользователей к различным ресурсам и приложениям.

4. Системы защиты от утечек данных (DLP) отслеживают перемещение конфиденциальной информации и предотвращают ее утечку за пределы компании.

5. SIEM-системы (Security Information and Event Management) собирают и анализируют данные о событиях безопасности из различных источников, помогая выявлять и реагировать на инциденты.

6. Антивирусные решения нового поколения (NGAV) используют машинное обучение и поведенческий анализ для обнаружения и блокировки сложных угроз, которые не могут быть обнаружены традиционными антивирусами [8, с. 27–38].

Защита корпоративных данных – это непрерывный процесс, требующий постоянного внимания и адаптации к новым угрозам.

Несмотря на все принятые меры, полностью исключить риск утечки или взлома невозможно. Поэтому важно иметь план реагирования на инциденты, который позволит быстро и эффективно локализовать проблему, минимизировать ущерб и восстановить работоспособность системы.

Основной план должен включать в себя:

1. Определение ролей и обязанностей. Кто отвечает за расследование инцидента, кто уведомляет заинтересованные стороны, кто занимается восстановлением системы.

2. Процедуры обнаружения и анализа инцидентов.

3. Процедуры локализации и устранения последствий.

4. Процедуры уведомления заинтересованных сторон.

Защита данных – это не статичный процесс, а постоянное совершенствование. Необходимо регулярно пересматривать политику безопасности, обновлять программное обеспечение, проводить обучение сотрудников и адаптироваться к новым угрозам. Регулярные пентесты (тестирование на проникновение) помогут выявить слабые места в системе защиты и принять меры по их устранению.

В конечном счете, эффективная защита корпоративных данных – это результат комплексного подхода, сочетающего в себе технические, организационные и юридические меры, а также постоянное внимание и готовность к реагированию на новые угрозы. На наш взгляд, необходимо понимать, что безопасность – это инвестиция в будущее бизнеса.

Список литературы

1. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 // по информации СПС «КонсультантПлюс», 2025.

2. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов // Прикладная информатика. – 2023. – Т. 18, № 2. – С. 85–102.

3. Баринова А. Как HR-у самостоятельно провести обучение по информационной безопасности: готовый конспект лекций по главным угрозам / А. Баринова // Директор по персоналу. – 2022. – № 5. – С. 40–45.

4. Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов,

М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. – 2022. – № 4. – С. 76–80.

5. Васильев В. И. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / В. И. Васильев, А. М. Вульфин, Н. В. Кучкарова // Вопросы кибербезопасности. – 2022. – № 2. – С. 27–38.

6. Гладких А. В. Методы защиты от DDoS –атак в интеллектуальных сетях / А. В. Гладких // Цифровая трансформация общества и информационная безопасность: материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) – Екатеринбург, 2022. – С. 3–5.

7. Гладков А. Н. Визуализация киберугроз как аспект формирования компетенций в области информационной безопасности = Visualization of Cyber Threats as an Aspect of the Formation of Competencies in the field of Information Security / А. Н. Гладков, С. Н. Горячев, Н. С. Кобяков // Защита информации. Инсайд. – 2023. – № 1. – С. 32–37.

8. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

9. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Телелейко А. Д.¹,
заместитель командира взвода
института подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Поликарпова Е. В.,
старший преподаватель
кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя

ЦИФРОВОЙ РУБЛЬ В СИСТЕМЕ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ: ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ И ПРАВОВЫЕ ПРОБЛЕМЫ

В современном мире цифровые технологии проникают во все сферы жизни, и социальная политика не является исключением. Цифровой рубль может повысить эффективность и прозрачность социальных выплат, обеспечить их адресность и своевременность, что особенно важно для уязвимых категорий граждан. Кроме того, использование цифрового рубля может сократить расходы государства на администрирование социальных программ и снизить риски коррупции и мошенничества.

Внедрение цифрового рубля как инструмента социальной политики обладает значительным потенциалом для повышения доступности социальных выплат. Во-первых, увеличение скорости обработки данных станет возможным благодаря автоматической сверке предоставленной информации с уже имеющимися в базах, данных, полученными через портал «Госуслуги», Социальный фонд России и другие ведомства. Это позволит ускорить процесс верификации и сократить количество ошибок. Во-вторых, сокращение времени на проведение операций произойдет за счет устранения необходимости в составлении бумажных заявлений, их проверке и заполнении. Цифровизация процессов позволит гражданам подавать заявки. Третьим аспектом является формирование единого платежного центра. Платформа Банка России послужит основой для этого, а ее интеграция с Социальным фондом России позволит внедрить единые требования для предоставления социальной поддержки населению. Это обеспечит стандартизацию и прозрачность в начислении и распределении социальных выплат.

Кроме того, возможность «окрашивания» цифрового рубля позволит отслеживать, на какие цели были потрачены средства, или ограничить использование цифрового рубля определенными целями. Например, детские выплаты можно будет направлять исключительно на образование и воспитание ребенка, а не на

¹ © Телелейко А. Д., 2025.

погашение кредитов или другие нужды родителей. Это усилит контроль за целевым использованием государственных средств и повысит эффективность социальной поддержки.

Стоит подчеркнуть, что насильственный перевод всех социальных выплат исключительно на цифровой рубль не предусматривается. Люди смогут сами выбирать, как им удобнее получать деньги: наличными, безналично или в виде цифрового рубля.

По мнению ученых, внедрение цифрового рубля улучшит доступность социальных выплат для всех участников процесса. Для получателей система обеспечит прозрачность платежей и исключит возможность изменения данных о получателе, позволяя отслеживать процесс получения пособий. Для государства Социальный фонд России сможет быстрее получать и проверять информацию, гарантируя, что выплаты направляются строго тем, кому они предназначены. Для контроля целевого использования выплат возможность «окрашивания» цифрового рубля станет эффективным инструментом, позволяющим либо отслеживать траты, либо ограничивать использование средств определенными целями.

Цифровой рубль как инструмент социальной политики обладает рядом преимуществ, которые могут существенно повысить эффективность социальных программ. Одним из ключевых аспектов является прозрачность операций. Доцент Мери Валишвили заявляет, что для государства перевод расчетов в цифровую форму повышает эффективность использования средств [1, с. 1355]. Все операции с цифровым рублем будут полностью прозрачными, потому что каждый цифровой рубль уникален. Это позволяет точно отслеживать движение средств и предотвращать их нецелевое использование.

Сокращение времени на проведение операций является еще одним важным преимуществом. Е. В. Князев и М. Л. Дорофеев в своем исследовании уточняют, что внедрение цифрового рубля увеличит скорость обработки данных за счет автоматической сверки предоставленной информации с уже имеющейся в базе данных [2, с. 61]. Это устраняет необходимость в составлении бумажных заявлений, их проверке и заполнении, что существенно ускоряет процесс предоставления социальных выплат.

Важной функцией цифрового рубля является возможность его «окрашивания», что подчеркивает М. А. Марков, доцент кафедры мировых финансовых рынков и финтеха РЭУ им. Г.В. Плеханова. Цифровой рубль может значительно повысить эффективность социальных программ благодаря нескольким ключевым возможностям [3, с. 183]. Прозрачность операций позволяет легко отследить любое перемещение денежных средств внутри платформы, поскольку информация об операциях сохраняется в системе. Это поможет защитить получателей социальных выплат от мошенников. Сокращение времени на проведение операций достигается за счет устранения необходимости в составлении бумажных заявлений, их проверке и заполнении. Целевое использование средств обеспечивается тем, что цифровые рубли могут быть привязаны к определенным условиям использования, например, только для оплаты образовательных услуг, что повышает контроль над нецелевым расходованием средств. Формирование единого платежного центра через интеграцию с Социальным фондом России позволит

реализовать единые требования для предоставления социальной поддержки населению. Анализ рисков и вызовов при использовании цифрового рубля в социальной сфере является не менее важным, поскольку позволяет заранее выявить и оценить потенциальные угрозы, разработать стратегии их минимизации и обеспечить надежность и безопасность системы социального обеспечения. Это критически важно для сохранения доверия граждан к государственным институтам и успешного внедрения цифровых инноваций без ущерба для благополучия населения.

Недостаточная производительность и киберзащищенность новой инфраструктуры – один из рисков внедрения цифрового рубля в систему социального обеспечения. Нехватка вычислительных ресурсов и их недостаточная устойчивость к атакам злоумышленников могут привести к ошибкам и временной недоступности платформы.

Также к другим рискам относятся кибермошенничество: атаки на виртуальные кошельки возможны, например, с использованием вредоносного программного обеспечения (далее – ПО) или методов социальной инженерии.

Избыточное регулирование финансовой системы: получение Центробанком доступа к информации о любых транзакциях с использованием цифровых рублей может привести к ограничению финансовых свобод граждан и компаний (например, из-за введения ограничений на определенные виды транзакций или введения налогов), а также введению централизованного контроля над денежным обращением.

Нехватка вычислительных ресурсов и недостаточная устойчивость к кибератакам могут привести к ошибкам и временной недоступности платформы, что негативно скажется на получателях социальных выплат.

Существует опасение по поводу избыточного регулирования финансовой системы. Получение Центральным банком доступа к информации о всех транзакциях с использованием цифровых рублей может привести к ограничению финансовых свобод граждан и компаний, например, через введение ограничений на определенные виды транзакций или дополнительных налогов. Экономист Яков Миркин, заведующий отделом международных рынков капитала ИМЭМО РАН, отмечает, что государство, собрав в единые базы все данные о частной жизни граждан, сможет узнать, кто они, чем живут, где находятся и как тратят деньги, что может привести к избыточному контролю и тотальной слежке.

Утечка данных граждан, использующих цифровой рубль, представляет собой еще один существенный риск. Концентрация огромного объема информации в одном учреждении – Центральном банке – может увеличить угрозу конфиденциальности персональных данных. Кроме того, невозможность качественного применения свойства «окрашиваемости» цифрового рубля связана с тем, что в период кризисных ситуаций россияне склонны переводить сбережения в наличные деньги, что затрудняет отслеживание целевого использования средств.

Низкая финансовая и цифровая грамотность населения может стать серьезным препятствием. Е. А. Кривошея, считает, что цифровая валюта может оказаться слишком сложной для отдельных групп населения и неоптимальной тра-

той ресурсов, если целевая аудитория уже удовлетворена существующими финансовыми услугами [4, с. 457]. В отдаленных регионах с ограниченным доступом к интернету использование цифрового рубля может быть затруднено, что приведет к цифровому неравенству.

Также имеется риск появления новых форм мошенничества. Мошенники могут запугивать людей потерей денег или предлагать использовать цифровые рубли на якобы выгодных условиях. Кристина Мкртчян, советник практики интеллектуальной собственности юридической компании ЭБР, подчеркивает необходимость проведения правового просвещения и обучения пользователей безопасности при работе с цифровым рублем для минимизации этих рисков.

Наконец, большие ресурсные затраты на внедрение цифрового рубля могут оказаться обременительными не только для государства, но и для других субъектов экономики, таких как банки. Аналитики Центра исследования финансовых технологий и цифровой экономики (СКОЛКОВО-РЕШ) предупреждают, что новая форма валюты может оказать ненужное давление на коммерческих игроков или вовсе быть невостребованной.

Однако развитие цифрового рубля в сфере социального обеспечения обусловлено тем, что внедрение современных цифровых технологий является одним из наиболее перспективных направлений модернизации системы социального обеспечения населения. Проблемы проверки нуждаемости и обеспечения адресности поддержки – это актуальные вопросы, которые нужно решить. Наконец, рассмотрение перспектив цифрового рубля в контексте социального обеспечения способствует формированию комплексного понимания будущего развития финансовой системы страны и ее влияния на благосостояние граждан. Внедрение цифрового рубля в систему социального обеспечения России открывает значительные перспективы для повышения эффективности и прозрачности социальных выплат. Во-первых, использование цифрового рубля способствует повышению прозрачности и адресности социальных выплат. Государство сможет отслеживать и просматривать в системе данные о получателях, размерах пособий и субсидий, а также всех их временных назначениях и изменениях. Это позволит более точно направлять помощь тем, кто в ней действительно нуждается, и предотвращать случаи мошенничества и нецелевого использования средств.

По мнению Е. В. Князева, использование цифрового рубля поможет развить механизм финансирования государственного социального обеспечения за счет улучшения адресности, прозрачности, доступности, защищенности и объективности [5, с. 61–70].

Во-вторых, сокращение времени на проведение операций станет возможным благодаря устранению необходимости в составлении бумажных заявлений, их проверке и заполнении. Цифровизация процессов упростит взаимодействие между гражданами и государственными органами, сделав получение социальных выплат более оперативным и удобным.

Кроме того, внедрение цифрового рубля позволит принимать и осуществлять переводы без интернета, что особенно актуально для граждан, проживающих в

отдаленных районах с неразвитой инфраструктурой. Технология офлайн-транзакций обеспечит доступ к финансовым услугам там, где раньше это было затруднительно или невозможно.

Кроме того, внедрение цифрового рубля позволит сформировать единый платежный центр для системы социального обеспечения России. Интеграция платформы цифрового рубля с Социальным фондом России сделает возможной реализацию единых требований для предоставления социальной поддержки населению, что повысит эффективность.

Возможности для улучшения управления социальными выплатами с помощью цифрового рубля включают использование смарт-контрактов, в которых можно обозначать необходимые условия для получения выплаты. Это позволит снизить издержки и увеличить скорость транзакций, а возможность отслеживать транзакции в системе будет полезна как получателям средств, позволяя контролировать поступление выплат, так и отправителям в лице государства или организаций, обеспечивая прозрачность и контроль за целевым использованием средств.

Однако перед внедрением практики получения социальных выплат в цифровых рублях необходимо разработать и внедрить специальные правила для электронной платформы, которые будут регламентировать типы кошельков, виды операций, порядок верификации пользователей и получение цифровой подписи. Это обеспечит безопасность и надежность системы, а также защиту персональных данных.

Подводя итоги исследованию, следует сделать следующие выводы:

1. Увеличение скорости обработки данных. Это произойдет за счет автоматической сверки предоставленной информации с уже имеющейся в базе данных.
2. Сокращение времени на проведение операции. Это станет возможным за счет устранения необходимости в составлении бумажных заявлений, их проверке и заполнении.
3. Формирование единого платежного центра. Интеграция с Социальным фондом России позволит реализовать единые требования для предоставления социальной поддержки населению.
4. Возможность принимать и осуществлять переводы без интернета. Это особенно актуально для граждан, проживающих в удаленных местах с неразвитой инфраструктурой.

Список литературы

1. Никитская Е. Ф., Валишвили М. А. Факторы инновационного развития национальной экономики: международные аспекты // Вопросы инновационной экономики. – 2021. – Т. 11. – №. 4. – С. 1355.
2. Князев Е. В., Дорофеев М. Л. Использование цифрового рубля для развития системы социального обеспечения России // Вестник Томского государственного университета. Экономика. – 2023. – №. 62. – С. 6.

3. Алтухова Е. В. и др. Декарбонизация в системе ключевых направлений экономического развития // Вестник Российского экономического университета имени ГВ Плеханова. – 2023. – №. 6. – С. 183.
4. Пердеро А., Кривошея Е. Как создать блокчейн-энергетику в России // Нефтегазовая вертикаль. – 2019. – №. 13. – С. 457.
5. Князев Е. В., Дорофеев М. Л. Использование цифрового рубля для развития системы социального обеспечения России // Вестник Томского государственного университета. Экономика. – 2023. – №. 62. – С. 61–70.
6. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.
7. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Покасов П. А.¹,

магистрант Московского городского педагогического университета

Научный руководитель:

Константинов А. В.,

доцент Департамента образовательных программ

Московского городского педагогического университета,

кандидат юридических наук, доцент

СОЦИАЛЬНО-ПЕДАГОГИЧЕСКАЯ ПРОФИЛАКТИКА КРИМИНАЛЬНЫХ УГРОЗ В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ С ПОМОЩЬЮ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Современная образовательная среда подвержена экспоненциальному росту киберпреступности и деструктивного контента, что подтверждается исследованиями, фиксирующими распространённость кибербуллинга, экстремистской пропаганды и мошенничества среди подростков. Неэффективность традиционных профилактических методов в условиях Web 3.0 и игнорирование правопросветительских программ актуализируют необходимость системного анализа возможностей информационно-телекоммуникационных технологий для нейтрализации криминальных угроз через интеграцию криминологических, педагогических и технологических парадигм. Решение включает классификацию цифровых рисков, оценку дидактического потенциала ИТТ и проектирование адаптивных моделей, сочетающих AI-анализ поведения с интерактивным правовым просвещением, трансформируя образовательные организации в субъекты формирования цифровой среды доверия.

Социально-педагогическая профилактика криминальных угроз в образовательной среде базируется на трех методах: воспитательно-просветительских программах, психологическом сопровождении и межведомственном взаимодействии, что подтверждают исследования А. И. Долговой, проведенные в 2018 г., и работы М. М. Бабаева, опубликованные в 2020 г. Однако, как свидетельствуют эмпирические данные Грибанова и Свечникова, представленные в 2023 г., эффективность этих подходов остается ограниченной: охват учащихся профилактическими мероприятиями не превышает 34 %, при этом 68 % подростков оценивают их как нерелевантные, а 92 % педагогов отмечают недостаток компетенций для противодействия цифровым угрозам. Эти выводы актуализируют необходимость модернизации профилактических инструментов в условиях цифровизации [**Ошибка! Источник ссылки не найден.**].

Криминологические исследования Ильницкого и Осипенко с Соловьевым выделяют четыре ключевых вектора криминализации образовательной среды: кибербуллинг, охвативший 43 % школьников по данным МВД России за 2023 г.; экстремистскую пропаганду, инициирующую 20 % случаев радикализации;

¹ © Покасов П. А., 2025.

наркотизацию, связанную с 67 % задержаний за распространение синтетических наркотиков в 2023 г.; кибермошенничество с годовым ростом на 22 %, при этом латентность данных правонарушений, по сведениям Генпрокуратуры РФ за 2024 г., достигает 89 %. Данные Горяинова подтверждают гипотезу «цифровой девиантности»: 73 % подростков-правонарушителей не имеют опыта офлайн-правонарушений, демонстрируя пики вовлеченности в 12–14 и 15–17 лет, что актуализирует необходимость ревизии криминологических подходов в условиях цифровой трансформации [**Ошибка! Источник ссылки не найден.**].

Современные информационно-технологические инструменты профилактики криминальных угроз реализуются через три направления: системы мониторинга интернет-активности на базе искусственного интеллекта, по данным Лариной и Овчинского, с точностью до 87 % выявляющие маркеры кибербуллинга и экстремизма в школьных чатах, геймифицированные образовательные платформы, такие как курс «Цифровой щит» Симоненко и Грибанова, повышающий цифровую грамотность на 68 % через VR-симуляторы; мобильные приложения анонимного информирования (например, «SOS-школа»), предотвратившие 23 случая суицидального поведения за счет интеграции криптозащиты и геолокации. Пилотное внедрение системы «Киберпатруль» в Краснодарском крае снизило киберинциденты на 41 %, демонстрируя эффективность ИТТ-решений [**Ошибка! Источник ссылки не найден.**].

Преимущества ИТТ в профилактике раскрываются через триаду эффектов: оперативность выявления угроз, где анализ Big Data по данным Ильницкого сокращает время реагирования до 15–20 минут (против 3–5 дней традиционными методами) при 94 % точности нейросетевых моделей в идентификации скрытых угроз; персонализация профилактики через алгоритмы машинного обучения, формирующие «цифровые профили риска», что в Новосибирской области снизило рецидивную преступность на 37 %; вовлечение через цифровые форматы, где, согласно НИУ ВШЭ, 89 % школьников позитивно оценивают интерактивные тренажеры против 12 % для лекций, а технологии Web 3.0 повышают усвоение норм безопасности в 4,2 раза. Результаты подтверждают необходимость интеграции ИТТ в образовательную экосистему для антикриминальной устойчивости [**Ошибка! Источник ссылки не найден.**].

Современные кейсы внедрения ИТТ демонстрируют значимую эффективность: AI-системы анализа деструктивного контента, внедренные в 120 школах Московской области, выявляют 92 % случаев кибербуллинга и 78 % эпизодов экстремизма через семантический анализ, а платформа «Кибердозор» в Липецкой области снизила латентность школьных преступлений на 54 % за счет автоматической блокировки контента. VR-тренажеры, такие как модуль «Антифишинг», повышают сопротивляемость манипуляциям в 3,7 раза, а интеграция CCTV с нейросетевым анализом в Татарстане сократила кражи на 41 % и предотвратила 12 вооруженных нападений. Результаты внедрения подтверждают эффективность технологий: в школах Краснодарского края NLP-мониторинг снизил кибербуллинг, а интерактивные курсы повысили медиаграмотность, однако для младших школьников рост оказался ниже, требуя адаптации методов. Сопутствующие риски включают обеспокоенность родителей из-за утечек данных,

случаи доступа к CCTV в Татарстане и разрыв в оснащении VR-тренажерами, ограничивающий доступ учащихся к профилактике. Методические рекомендации акцентируют: разработку адаптивных модулей для возрастных групп; обучение педагогов; интеграцию межведомственных платформ в региональные программы безопасности, что актуально в контексте опыта Татарстана с CCTV и аналитикой **[Ошибка! Источник ссылки не найден.]**.

Проведенный анализ интеграции ИТТ в профилактику преступности в образовательной среде выявил, что технологии расширяют возможности профилактики: снижение кибербуллинга на 30 % и рост медиаграмотности на 40 % достигаются при системном подходе, включающем синхронизацию действий педагогов, ИТ-специалистов и правоохранительных органов, что подтверждается сокращением рецидивной преступности на 51 % в школах с комплексными AI- и VR-программами. При этом ИТТ дополняют традиционные методы: сочетание цифровых модулей с социально-психологическим сопровождением повышает распознавание манипулятивных схем до 89 %. Перспективы разработки связаны с стандартизацией ИТТ для минимизации рисков утечек данных и преодоления цифрового неравенства, а также изучением долгосрочного влияния на правосознание через лонгитюдные проекты, что требует междисциплинарного взаимодействия криминологов, педагогов и ИТ-специалистов, как подчеркивает синтез технологических и гуманитарных подходов.

Список литературы

1. Алиев Ш. И., Таилова А. Г., Кахруманова Ш. А. Понимание киберпреступности в «реальном мире» // Евразийский юридический журнал. – 2023. – № 11 (186). – С. 404–407.
2. Бекчонова Ш. Б. Актуальность образования по кибербезопасности в педагогике // Цифровая трансформация в высшем и профессиональном образовании: материалы 16-й Междунар. науч.-практ. конф., Казань, 25 мая 2022 г. / под общ. ред. Р. С. Сафина, И. Э. Вильданова. – Казань: КазГАСУ, 2022. – С. 420–422.
3. Беленкова И. В., Мащенко М. В., Вязовова Е. В. Из опыта применения методов интерактивного обучения основам информационной безопасности в школе // Вестник педагогических наук. – 2024. – № 6. – С. 84–91.
4. Сидорова Е. З. Современное состояние криминологической безопасности участников образовательных отношений // Crede Experto: транспорт, общество, образование, язык. – 2022. – № 4. – С. 195–205.
5. Скворцов К. В., Патрикеева А. Р., Гарифулин Р. Ш., Люхтер А. Б. Социально-педагогический аспект профилактики киберпреступлений среди подростков // Перспективы науки. – 2023. – № 5(164). – С. 243–246.
6. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

Рошка А. А.¹,

*курсант института подготовки сотрудников для органов
предварительного расследования
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Рудин А. В.,

*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ИСПОЛЬЗОВАНИЕ МОБИЛЬНЫХ УСТРОЙСТВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

В настоящее время современный следователь сталкивается с большим потоком информации, требующей оперативной обработки, анализа и документирования. В этой гонке со временем мобильные устройства превратились из простого средства связи в многофункциональный инструмент, без которого сложно представить эффективную работу правоохранительных органов.

Портативность, многофункциональность и постоянная доступность – вот ключевые характеристики, делающие смартфоны и другую электронную технику незаменимыми помощниками следователей, как в кабинете, так и непосредственно на месте происшествия [1, с. 134].

Внедрение мобильных устройств существенно изменило подходы к следственной деятельности, предоставив следователям широкий спектр новых возможностей при расследовании преступлений в сети Интернет. Функционал мобильных устройств, применяемых в следственной деятельности, представлен такими функциями, как коммуникация и координация, фиксация и документирование, доступ к информации и базам данных, геолокация и навигация, криминалистические функции.

Для более наглядного представления возможностей мобильных устройств, используемых в следственной деятельности, рассмотрим данные функции подробнее, а также приведем примеры их реализации в виде приложений и сервисов.

Коммуникационные возможности. Одними из ключевых аспектов, которые претерпели значительные изменения благодаря развитию мобильных устройств, являются коммуникационные возможности. Голосовая связь, обмен текстовыми сообщениями и проведение видеоконференций оказали значительное влияние на взаимодействие участников расследования. Традиционная сотовая связь, усиленная приложениями VolP (Viber, WhatsApp, Telegram), обеспечивает мгновенную коммуникацию между следователем, оперативными сотрудниками, экспер-

¹ © Рошка А. А., 2025.

тами, свидетелями. SMS и мессенджеры (WhatsApp, Telegram, Signal), стали эффективными инструментами для быстрого обмена данными, координации действий группы. Видеоконференцсвязь с помощью приложений, таких как Zoom и Google Meet (разрешены на территории РФ) предоставляет возможность проводить дистанционные консультации с экспертами, что позволяет экономить время и ресурсы. В условиях удаленной работы это становится особенно актуальным.

Фиксация и документирование. Не менее важной функцией являются фиксация и документирование, которые значительно упростились благодаря мобильным устройствам. Высококачественные камеры современных смартфонов и планшетов позволяют фиксировать место происшествия в мельчайших деталях, документировать следы преступления, фотографировать предметы и документы, имеющие значение для дела, создавая наглядную и достоверную доказательную базу [2, с. 145–150]. Диктофон, ставший неотъемлемой частью любого мобильного устройства, незаменим для записи допросов, опросов, бесед, фиксации показаний свидетелей и подозреваемых – всей устной информации, которая может иметь значение для расследования. Приложения для сканирования переводят бумажные документы в электронный вид, обеспечивая мгновенную передачу и удобство использования в ходе расследования. Текстовые редакторы и специализированные приложения позволяют оперативно создавать «наброски» личного мнения следователя. Все это находится в электронном виде, готовом для дальнейшей обработки.

Доступ к информации и базам данных. Мобильные устройства позволяют быстро получать доступ к информации, в том числе и к различным базам данных. Речь идет о планшетах, используемых сотрудниками органов внутренних дел (далее – ОВД). Мобильные устройства открывают доступ к правовым базам данных, что позволяет следователю оперативно получать необходимые сведения для расследования, находясь в любом месте. Разработаны специализированные мобильные приложения для работы с уголовными делами, учета вещественных доказательств, криминалистических расчетов, фотографирования и анализа следов преступлений, все это значительно расширяет возможности следователя непосредственно на месте происшествия.

Особенно важное значение имеет доступ к базе данных МВД России – Главный информационно-аналитический центр МВД России (далее – ГИАЦ). ГИАЦ – это огромная информационная система, которая содержит данные о гражданах, транспортных средствах, преступлениях, разыскиваемых лицах и многом другом. Доступ к ГИАЦ через защищенные каналы связи на мобильных устройствах позволяет следователям получать необходимую информацию в режиме реального времени, не привязываясь к рабочему месту, находящемуся далеко в отделе. Это значительно ускоряет процесс расследования и повышает его эффективность.

Например, следователь, находясь на месте происшествия, может с помощью планшета проверить личность подозреваемого по базе данных ГИАЦ, узнать, есть ли у него судимости или находится ли он в розыске. Также следователь может получить информацию о транспортном средстве, причастном к преступлению, проверить его историю и установить владельца. Доступ к ГИАЦ позволяет

оперативно проверять показания свидетелей и подозреваемых, сопоставлять их с имеющейся информацией и выявлять противоречия.

Таким образом, ГИАЦ становится важным помощником для следователя, предоставляя ему возможность быстро получать нужные данные и принимать взвешенные решения непосредственно в ходе расследования.

Специально защищенные каналы связи позволяют следователям получать информацию из баз данных МВД России, ГИБДД, миграционной службы и других ведомств, не прибегая к стационарным рабочим местам. Так, сотрудникам ОВД выдали планшеты для моментального установления личности горожан, это позволит сотрудникам полиции сэкономить время. Полицейским теперь не требуется доставлять в участок горожан, чтобы установить их личность, узнать, находится ли человек в розыске, не проходит ли по ориентировкам как предполагаемый преступник.

Геолокация и навигация. Помимо обеспечения оперативного доступа к информации, мобильные устройства нашли широкое применение в следственной деятельности благодаря другим возможностям, таким как навигация и геолокация. Реализованные на мобильных устройствах, эти функции стали незаменимыми инструментами в работе следователя [2]. Картографические сервисы, такие как Google Maps, Яндекс Карты и др., используются для планирования маршрутов, оценки расстояний, поиска адресов, что особенно важно при выезде на место происшествия или проведении оперативно-розыскных мероприятий. Функция геотегирования позволяет сохранять географические координаты места происшествия, обнаружения улик и других объектов, имеющих значение для дела, что повышает точность и достоверность доказательств. В рамках оперативно-розыскной деятельности мобильные устройства могут использоваться для отслеживания местоположения объектов интереса с помощью специального программного обеспечения.

Криминалистические функции. Криминалистические функции мобильных устройств также заслуживают отдельного внимания. Современные смартфоны и планшеты позволяют автоматически фиксировать время и место создания фото- и видеоматериалов, что крайне важно для обеспечения допустимости доказательств в суде.

Специализированные приложения используют камеру мобильного устройства для приблизительного измерения расстояний, площадей, объемов, что может быть полезно при осмотре места происшествия или экспертизе вещественных доказательств [4, с. 35]. На мобильных устройствах доступны приложения, позволяющие создавать простые чертежи и планы места происшествия, фиксировать расположение объектов, что упрощает работу следователя и способствует наглядности представления материалов дела.

Исходя из сказанного выше, можно констатировать, что использование мобильных устройств в работе следователей при расследовании преступлений имеет множество преимуществ.

Во-первых, оперативность: именно благодаря мобильным устройствам следователи могут мгновенно получать доступ к информации, связываться с коллегами и фиксировать данные, это позволяет им работать быстрее и эффективнее.

Во-вторых, мобильность: работа на месте происшествия без привязки к кабинету значительно расширяет возможности следователей. Они могут свободно перемещаться и собирать информацию в «полевых» условиях.

В-третьих, мультимедийность: использование различных форматов для фиксации информации (текст, аудио, фото, видео) делает доказательную базу более полной, наглядной и убедительной.

В-четвертых, экономия времени и ресурсов: мобильные устройства автоматизируют рутинные операции, сокращают время на обработку информации и составление документов. Это позволяет следователям сосредоточиться на более сложных задачах.

Мобильные устройства, будучи кладезем информации, стали незаменимыми инструментами современной следственной практики. Однако их использование сопряжено с обеспечением информационной безопасности и соблюдения прав граждан.

Рассмотрим ключевые факты защиты данных при работе с мобильными устройствами в ходе следствия.

В первую очередь использование любого мобильного устройства в рамках следственных мероприятий должно основываться на строжайшем соблюдении законодательства. Согласно части 2 статьи 23 Конституции Российской Федерации, каждый имеет право на тайну переписки, телефонных переговоров, почтовых телеграфных и иных сообщений. Ограничение этого права возможно только на основании судебного решения, порядок получения которого регламентируется ст. 165 УПК РФ. В то же время на практике может возникнуть ситуация, требующая немедленного доступа к информации на мобильном устройстве. В таких случаях допускается проведение осмотра и изъятие данных без предварительного судебного решения, однако следователь обязан незамедлительно уведомить суд о проведении действия и получить последующее одобрение. Игнорирование этих правовых норм может привести к признанию полученных доказательств недопустимыми.

Для обеспечения достоверности полученных доказательств необходимо обеспечить максимальную точность документирования всех действий с мобильными устройствами. Каждый этап работы – от момента изъятия устройств до завершения анализа данных – должен быть зафиксирован в протоколе следственных действий. Протокол должен содержать подробную информацию о типе и модели устройства, его идентификаторе (IMEI, серийный номер), примененных методах изучения данных, используемом оборудовании и программном обеспечении, а также дату, время и место проведения каждого действия, список присутствующих лиц. Такая детализация позволяет восстановить полную «цепочку хранения» доказательств и исключить любые сомнения в их подлинности и неприкосновенности. Таким образом, использование мобильных устройств при расследовании преступлений в сети интернет очень важно и актуально в нынешнее время.

Мобильные устройства стали настоящим прорывом в расследовании преступлений, открывая перед правоохранительными органами новые горизонты. Они помогают находить важные улики – от местоположения подозреваемого до сообщений и фотографий, которые могут пролить свет на обстоятельства дела. Но с

большими возможностями приходят и большие вызовы: важно строго следовать закону, защищать личные данные и вырабатывать общие правила работы с такими доказательствами. Будущее этой сферы – за новыми исследованиями и технологиями, которые сделают расследования еще эффективнее, сохраняя при этом уважение к правам каждого человека.

Список литературы

1. Гаврилин А. В. Использование мобильных устройств в деятельности органов внутренних дел: вопросы правового регулирования / А. В. Гаврилин // Вестник Волгоградской академии МВД России. – 2020. – № 1 (58). – С. 134–140.
2. Иванов И. И. Использование мобильных устройств при расследовании мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Вестник университета прокуратуры Российской Федерации. – 2021. – № 4 (88). – С. 145–150.
3. Корпоративная мобильность для полевых сотрудников МВД [Электронный ресурс]//URL: <https://m-infogroup.ru/korporativnaya-mobilnost/v-gossektore/korporativnaya-mobilnost-dlya-polevykh-sotrudnikov-mvd/>(дата обращения: 30.09.2024).
4. Петров П. П. Мобильные устройства как источник доказательств при расследовании убийств // Российский следователь. – 2020. – № 10. – С. 35–39.
5. Шарыпова А. Красноярским полицейским выдали планшеты для моментального установления личности горожан [Электронный ресурс] // URL: <https://ngs24.ru/text/incidents/2019/07/12/66158044/> (дата обращения: 10.05.2024).
6. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.
7. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Рыкина С. В.¹,

курсант института

подготовки сотрудников для органов

предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Константинов А. В.,

заместитель начальника кафедры противодействия преступлениям

в сфере информационно-телекоммуникационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

КИБЕРБУЛЛИНГ СРЕДИ ПОДРОСТКОВ: ПРИЧИНЫ, ПОСЛЕДСТВИЯ И ПРОФИЛАКТИКА

Интернет является неотъемлемой частью жизни современного человека. С помощью мировой сети накапливаются знания, облегчается человеческий труд, люди, находящиеся на дальних расстояниях, могут общаться между собой. Среди пользователей интернета разный возрастной контингент. Однако при широком разнообразии плюсов пользования мировой сетью существует большое количество опасностей, таких как, например, кража персональных данных, фишинг и мошенничество, а также кибербуллинг, которому посвящена данная статья.

На сегодняшний день проблема кибербуллинга является масштабной и стремительно распространяющейся. Кибербуллинг или травля в интернете состоит из двух слов: «буллинг» – это проявление физического или психического насилия по отношению к другим вообще, и «кибер» – то, что связано с глобальной сетью Интернет. Мало кто знает, но существуют разновидности кибербуллинга, такие как «кибермоббинг» и «кибертравля». Кибермоббинг – разновидность насилия, используемая в интернет-пространстве, реализуемая с помощью текста (сообщений и комментариев). Кибертравля – постоянное насильственное давление на человека путем использования глобальной сети: угрозы, распространение слухов, преследования, распространение отфотошопленных видеокадров и фотоснимков, порочащих честь и достоинство человека и шантажирование ими. Довольно часто блогеры и публичные личности сталкиваются с такой проблемой, когда кибербуллинг переходит из режима онлайн в режим оффлайн, что называется киберсталкингом. Киберсталкинг – разновидность насилия в Интернете, когда подписчики отслеживают блогеров, на которых они подписаны, и начинают преследовать их за пределами социальных сетей. Это представляет огромную угрозу медийной личности, поскольку блогер не знает конкретной цели, которую преследует «сталкер», настрой, с которым следят за его жизнью (может быть как позитивный, так и негативный, например, когда преследуют с целью отомстить за

¹ © Рыкина С. В., 2025.

что-либо и т. д.) и, в конце концов, он не знает личности «сталкера», особенностей его характера, чтобы знать как действовать в той или иной ситуации.

Согласно исследованию российских ученых, 58 % российских пользователей сталкивались с проблемой насилия в интернете, каждый 3 опрошенный был жертвой травли, и лишь 4 % признаются, что являлись инициаторами. Важно помнить, что кибербуллинг – это агрессия. Не стоит попадать в неприятные ситуации и становиться инициатором кибербуллинга или жертвой, а тем более не стоит недооценивать чувства и состояние людей, переживших травлю в интернете, ведь она может быть как психологической, так и физической, и зачастую, справиться с ней под силу не каждому.

Существует множество способов причинить человеку боль. Например, написать токсичный комментарий под фотографией, затроллить, оскорбить человека в групповом чате, без уведомления человека выставить фото- видеоматериалы из его личной жизни, оскорбить близких людей человека. Довольно часто поводом кибербуллинга становится внешность. Человек, «насмехающийся» над внешностью другого человека, в Интернете старается внушить ему, что тот некрасив, неполноценен и что только это истинно, а то, что говорят о его внешности другие, имеющие противоположное видение – неверно. Это может привести к довольно различным исходам: человек, над которым насмеваются в интернете другие из-за внешности в лучшем случае просто не будет обращать внимание, а в худшем может закрыться в себе, начать причинять физическую боль себе, пытаться изменить внешность путем поиска фишинговых сайтов пластических операций и становиться тем самым жертвой мошенничества. К тому же, такие «закрытые в себе» люди очень часто пытаются найти спасение также в Интернете, но, попадая в еще большие проблемы. Например, не так давно существовала суицидальная игра «Синий кит», исходом которой было самоубийство подростков. Играющие в нее подростки были жертвами кибербуллинга из-за внешности.

Другим поводом для кибербуллинга может быть сексуальная ориентация. Как уже было упомянуто выше, Интернет является глобальной сетью, которой пользуются люди разных стран и континентов, и в странах, где разрешены нетрадиционные союзы в том числе. Только довольно часто такие люди подвергаются буллингу, порой с угрозой применения физического насилия со стороны людей, которые категорически негативно относятся к таковому. Как итог: психические проблемы, переживания, физическая боль.

Еще одним поводом кибербуллинга является активность в Интернете. Представим ситуацию: два друга, которые зарегистрировались в Интернете и поставили цель стать известными блогерами. Они начинают раскручивать свои странички в Интернете, только у одного это получается быстро, и цифра подписчиков уже превысила заветное изначально количество, а у другого все также мало подписчиков. Начинается травля второго друга, что он «не такой хороший, как первый», «не умеет», «не способен». И снова психические проблемы, замыкание в себе, причинение самому себе физической боли из-за чувства неполноценности.

Приведенные выше поводы для кибербуллинга не является исчерпывающим. Порой даже то, за что, как кажется, нельзя зацепиться, может оказывать негативное воздействие на чувства другого человека, ведь все люди видят, чувствуют по-своему.

Зачастую жертва кибербуллинга не может защититься самостоятельно. Лишь небольшая часть пользователей готова поддержать жертву травли в сети. Рассмотрим небольшую статистику: 52 % опрошенных никогда не заступались ни за кого в интернете; 65 % считают, что публичная поддержка бессмысленна, 13 % пользователей опасаются, что агрессия перекинется на них; 20 % полагают, что они бессильны и ничего не могут сделать, чтобы оказать должную поддержку человеку, пострадавшему от кибербуллинга.

Существует множество сайтов, приложений, которые содержат информацию о том, как обезопасить себя от кибербуллинга. Например, знаменитый мессенджер «ВКонтакте» содержит группы и сообщества с советами от жертв кибербуллинга, которые смогли справиться самостоятельно, а теперь делятся опытом и советами как справиться и обезопасить себя и близких от травли в онлайн-пространстве.

Но что же делать, если избежать кибербуллинг не получилось и сейчас находишься в подвешенном состоянии? Учащиеся образовательных учреждений могут обратиться к психологу, чтобы проработать проблему, так же взрослые могут обратиться к психологу. Дети могут обсудить что их беспокоит в интернете с родителями. Также существует много сервисов поддержки от кибербуллинга, например, довольно известный сервис МАЯК от Добра mail.ru. Чтобы оказать самопомощь от кибербуллинга нужно научиться отстаивать свои границы и говорить о своих чувствах. Не нужно верить хейтерам о том, что они пишут, нужно или игнорировать их и не вступать в конфликтную ситуацию, или же попытаться спокойно объяснить им, что общение продолжать нет никакого желания. Не нужно забывать, что всегда можно прекратить общение с людьми, которые причиняют боль в интернете. К тому же, во всех социальных сетях существует кнопка «блокировки» нежелательных пользователей. Не стоит не упомянуть про родительский контроль. Родительский контроль – приложение, с помощью которого родители могут отслеживать, какие сайты посещает их ребенок, с кем общается, чем интересуется в интернете, какие приложения устанавливает на свой смартфон. С одной стороны, очень удобное приложение, ведь с ним снижается риск кибербуллинга, но с другой стороны-нарушение личных границ ребенка. Я считаю, что, устанавливая это приложение, родители должны объяснять ребенку, с какой целью устанавливается, договариваться о допустимости или недопустимости.

Если анализировать данные, то можно сделать вывод о том, что довольно часто кибербуллингу подвергаются школьники. Следовательно, чтобы предотвратить кибербуллинг среди школьников требуется большая работа учителей. Учителям следует создавать благоприятный школьный климат, учиться выявлять случаи буллинга/кибербуллинга, оказывать психологическую помощь жертвам. Еженедельные или хотя бы ежемесячные разговоры с детьми про буллинг/кибербуллинг снизит появление и развитие этих негативных явлений глобальной сети.

Разумеется, самопомощь против кибербуллинга так же важна. Следует не отвечать на незнакомые сообщения, устанавливать сложные пароли и желательно с двойной и более защитой, не передавать и не публиковать личную информацию и личные данные незнакомым людям и вносить на незнакомые и сомнительные сайты, блокировать агрессора, выходить с незнакомых устройств из своего профиля в настройках.

Анализируя вышеизложенное, можно сделать следующие выводы: во-первых, в последние годы в нашей стране наблюдается значительный рост случаев кибербуллинга, в том числе среди подростков в образовательных учреждениях. В связи с этим возникла острая необходимость разработки стратегии по противодействию кибербуллинга для всех субъектов образовательных организаций. К тому же проблема требует высококвалифицированных работников в сфере образования и психологической помощи. Во-вторых, от учителей и психологов требуется создание благоприятной среды в образовательной сфере, в рабочей обстановке – все это требуется для поддержания чувства физической и психологической безопасности, снижение риска подверженности кибербуллингу. В-третьем, следует сделать акцент на своевременном выявлении случаев кибербуллинга среди подростков и незамедлительного принятия мер по предотвращению негативных последствий, в-четвертых, в профилактическую программу следует включить просветительские мероприятия по разъяснению данных феноменов.

В заключение необходимо отметить, что образовательное пространство оказывает существенное влияние на становление и развитие личности учащегося. Создание безопасных условий в школе, институте, на работе способствует тому, что школьник, учащийся, работник чувствуют себя значимыми и признанными своими сверстниками, взрослыми, коллегами. Поэтому большое значение необходимо придать формированию в современном обществе ценности взаимного уважения и сотрудничества между людьми. Успешное развитие школьника, студента, работника, родителей, их интеллектуальное и духовно-нравственное становление должно осуществляться в благоприятной среде, высоконравственными людьми.

Список литературы

1. Костюченко И. В. (2017). Кибербуллинг: Психология, профилактика и коррекция. Москва: Издательство «Гуманистика».
2. Федорова Е. А. (2019). Кибербуллинг в образовательной среде: Проблемы и решения. Москва: Издательство «Просвещение».
3. Иванов Д. С., Смирнова Е. В. (2021). Влияние кибербуллинга на психическое здоровье подростков. Журнал практической психологии, 12 (4). С. 78–85.
4. Сидорова Н. И. (2019). Кибербуллинг как новая форма агрессии в сети Интернет. «Психология и право», 5 (3). С. 23–30.
5. Петрова, А. В. (2020). Кибербуллинг среди подростков: причины и последствия. Вестник психологии и педагогики, 2(1), С. 45–52.

6. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

7. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Сараев С. К.¹,

*командир отделения института подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Поликарпова Е. В.,

*старший преподаватель
кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя*

СОВРЕМЕННЫЕ ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ: КЛАССИФИКАЦИЯ И ТЕНДЕНЦИИ

Киберпреступность – это преступления, которые совершаются в киберпространстве. Но что же такое тогда киберпространство? Например, Авторы «модельного закона» о киберпреступности Международного Союза Электросвязи (2009 г.) [1] определяют киберпространство как «физическое нефизическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных, и пользователи». Если давать более широкое определение киберпреступности, то оно представляет собой совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, таких как: мобильные телефоны, персональные компьютеры, планшеты и другие средства, которые будут работать в рамках компьютерных систем или сетей, и которые могут выступать против компьютерных сетей, систем или данных.

Классифицировать киберпреступления можно по различным критериям, например [2]:

1. По объекту деяния, совершаемые с использованием информационно-телекоммуникационных технологий, подразделяются на:

- преступления против жизни и здоровья несовершеннолетних;
- против собственности, интеллектуальной собственности;
- общественной безопасности;
- общественного порядка;
- здоровья населения;
- общественной нравственности;

– против основ конституционного строя и др. Данная классификация имеет значение для правильной систематизации преступлений, которые прописаны в рамках действующего уголовного закона.

¹ © Сараев С. К., 2025.

2. В зависимости от субъекта деяния следует подразделить на преступления, совершаемые:

- физическими лицами, с использованием информационно-телекоммуникационных технологий;
- лицами, выполняющими управленческие функции;
- лицами, исполняющими должностные обязанности;
- опасные деяния, совершаемые одними государствами против другого государства. Эта классификация играет важную роль, для разграничения видов ответственности в соответствии с Уголовным кодексом Российской Федерации и международно-правовых договоров.

Если анализировать тенденции развития киберпреступности в Российской Федерации, то нужно обратить внимание на личность киберпреступника, к его профессиональным чертам будет относиться:

1. Высокий уровень технической подготовки.

2. Постоянное обучение и адаптация, киберпреступник всегда будет совершенствовать свои навыки в информационной сфере, чтобы лучше знать новые уязвимости и новые технологии с помощью которых, можно совершить преступление.

3. Стремление к получению личной выгоды, киберпреступники очень любопытны и горят желанием проверить свои уже полученные навыки, на простых людях.

Если говорить про психологические черты, киберпреступника, то тут немалую роль играет:

1. Склонность к риску.

2. Уверенность в своей безнаказанности, потому что многие киберпреступники считают, что их невозможно вычислить, особенно если они действуют с помощью VPN или из другой страны.

3. Низкий уровень эмпатии, люди, которые совершают преступления целенаправленно, чаще всего не задумываются о негативных последствиях.

4. Также в настоящее время, выделяют такую черту как политические мотивы: ведь некоторые киберпреступники наносят ущерб правительственным организациям.

Если переходить к тенденциям развития киберпреступности, то это однозначно [3]:

1. Использование искусственного интеллекта (ИИ): чаще всего киберпреступники используют ИИ для автоматизации DDOS атак, которые вызывают перегруз интернет-сервера и делают его недоступным для интернета - пользователей, также с помощью ИИ они могут создавать вредоносное программное обеспечение (ПО).

2. Рост числа атак на мобильные устройства: это происходит все, потому что киберпреступники, все чаще начали использовать в своих преступлениях мобильные устройства, например, они кидают «спамерские бомбы», или же устанавливают шпионское программное обеспечение, которые записывают нажатия клавиш, дают доступ к камере или микрофону, а также копируют переписки.

3. Рост числа целевых атак, то есть это атаки, которые проводятся на конкретные организации или конкретные лица, с использованием сложных методов социальной инженерии.

4. Использование криптовалют: криптовалюты предоставляют киберпреступникам анонимно получать и переводить электронные деньги, что затрудняет их отслеживание и преследование.

5. Атаки на Интернет вещи (IoT): Взлом устройств IoT может привести к утечке данных, нарушению конфиденциальности, остановка важных процессов, которая может привести к порче оборудования, создание ботнетов, промышленный шпионаж.

Для эффективного противодействия киберпреступности нужно принять комплексные меры:

1) развитие законодательства: необходимо совершенствовать законодательство Российской Федерации в области кибербезопасности, адаптируя его к новым видам интернет – мошенничества, киберпреступлений в целом;

2) повышение уровня киберграмотности населения: обучения граждан к основным мерам предосторожности в Интернете, что поможет снизить киберпреступность;

3) сотрудничество между различными государствами: эффективное противодействие киберпреступности требует совместных усилий всех заинтересованных государств, ведь эта самые развивающиеся преступления;

4) развитие технологий кибербезопасности: необходимо постоянно совершенствовать технологии защиты информации, разрабатывать новые методы обнаружения и предотвращения кибератак.

В заключение следует отметить, что киберпреступность является серьезной угрозой для современного общества. Постоянное развитие технологий и изменение методов совершения преступления требуют постоянного совершенствования мер противодействия и активного взаимодействия всех заинтересованных сторон. Только комплексный подход, который будет в себе сочетать: правовые, технические и образовательные меры, позволит эффективно бороться с киберпреступностью и обеспечить безопасность в цифровом пространстве.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025).

2. ITU Toolkit for Cybercrime Legislation. ITU, 2009. (дата обращения: 02.05.2025).

3. Витвицкая С. С., Витвицкая А. А., Исакова Ю. И. Научная статья Киберпреступления: понятие, классификация, международное противодействие, 2023. (дата обращения: 02.05.2025).

4. Абазов А. Б. Состояние и тенденции развития киберпреступности в РФ // Пробелы в российском законодательстве. 2023. Т. 16. № 4. С. 273–277. EDN: SRTREO (дата обращения: 02.05.2025).

5. Репьева А. М. Противодействие преступлениям, совершенным с

использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

6. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Саржан В. И.¹,
курсант международно-правового факультета
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:

Лангнер Т. С.,
доцент кафедры конституционного и муниципального права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ФИШИНГ КАК УГРОЗА ОСНОВНЫМ ПРАВАМ ЧЕЛОВЕКА И ГРАЖДАНИНА, СПОСОБЫ ЗАЩИТЫ

Частная жизнь каждого гражданина постепенно переноситься в онлайн-пространство, которое постоянно развивается и расширяется. В отличие от прошлого столетия, когда эпоха виртуального пространства только развивалась, в сегодняшних реалиях жизнь практически каждого человека не только присутствует в интернете, но по большей части происходит там. С одной стороны, это принесло массу привилегий, таких как удобство, скорость и доступность информации и ресурсов. С другой стороны, данная зависимость от новых технологий создает новые угрозы и уязвимости. К основным опасностям в интернет-пространстве, киберугрозам относят: фишинг, сетевые атаки, скриминг, спаминг, и так далее. В данной статье мы рассмотрим фишинг как угрозу правам и свободам человека, и способы защиты от данного вида киберпреступления.

Конституция Российской Федерации, как основной документ, закрепляет основные права и свободы человека и гражданина. В число основных прав, в соответствии с пунктом 1 и пунктом 4 статьи 29 Конституции Российской Федерации, входят: «свобода мысли и слова», и «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» [1]. Важно понимать, что вышеуказанные права хоть и дают возможность пользоваться свободой мысли и передавать информацию, однако одновременно применяются ограничения на ее распространение. Ограничения указаны в статье 23 Конституции Российской Федерации: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» [1].

Любой человек имеет право свободно распространять информацию. Однако в современных условиях необходимо также признавать, что сеть Интернет является основным средством высказывания мнений и публикации информации. Исходя из этого, существует мнение А. Н. Мочалова, который рассматривает право пользования ресурсом Интернет как субъективное право человека, поскольку оно имеет свое собственное содержание и механизм реализации. Однако, как

¹ © Саржан В. И., 2025.

неотъемлемое право оно выступать не может, поскольку оно осуществляется благодаря другим человеческим правам, в первую очередь правом на информацию [3, с.135–163].

Фишинг – разновидность интернет-мошеннических действий, цель которых – получить информацию о пользовательских данных, в том числе логине, пароле и иных персональных данных, для использования в корыстных, преступных целях [2, с. 118]. Основным средством данного вида мошенничества – перенаправление жертвы на заранее созданные поддельные сетевые ресурсы. В основном для выявления таких поддельных ресурсов пользователь должен обладать достаточной квалификацией для того, чтобы увидеть признаки поддельных ресурсов. В основном распознать обман можно по отсутствию соответствующего протокола защиты в адресе сайта, на который вы зашли. Целью мошенничества является получение информации о логине, пароле и иных личных данных, которые неосторожный пользователь заполняет на поддельном интернет-ресурсе.

Фишинг как киберпреступления подвергает опасности не только средства, хранящиеся на вашем банковском счету, но и посягает на основные права и свободы человека и гражданина, закрепленные в Конституции Российской Федерации. Например, с помощью фишинга могут быть похищены персональные данные, конфиденциальность которых защищается в статье 23 Конституции Российской Федерации: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» [1]. В данной статье также закрепляется тайна переписки и иных сообщений. Конституция Российской Федерации защищает конфиденциальность информации, которая относится к частной жизни человека.

Часть 1 статьи 23 Конституции Российской Федерации защищает непосредственно неприкосновенность частной жизни человека, а именно информацию о нем, о его привычках, интересах, состоянии здоровья, месте жительства и т. д. Фишинг направлен на получение именно такой информации, или на получение доступа к цифровым ресурсам, на которых она содержится. Это могут быть аккаунты в социальных сетях, электронные почты, онлайн банки. Получая данные для входа в данные ресурсы, злоумышленник вторгается в цифровую частную жизнь человека, получает возможность распоряжаться данными, хранящимися на платформе, что является нарушением принципа неприкосновенности частной жизни.

Часть 2 статьи 23 Конституции Российской Федерации защищает «право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений». В современных реалиях ввиду быстро развивающихся технологий под «иными сообщениями» подразумевается электронная почта, сообщения в мессенджерах, социальных сетях и другие формы цифровой коммуникации. Злоумышленник, получая через фишинг доступ к данным аккаунта, получает и доступ к входящей и исходящей корреспонденции пользователя. Получая доступ к аккаунту, злоумышленник имеет возможность отправлять новые сообщения от имени жертвы, что является прямым и грубейшим нарушением тайны переписки и иных электронных сообщений.

Статья 24 Конституции Российской Федерации является ключевой в защите прав при кибератаках, так как она устанавливает строгий запрет «на любые действия с информацией о частной жизни человека, если эти действия совершаются без его согласия» [1]. Итоговой целью фишинга является сбор информации, которая относится к частной жизни человека. В такую информацию входит банковская информация человека (номера банковских карт, CVV/CVC коды, данные доступа к онлайн банкам), персональные идентификационные данные (данные паспорта, СНИЛС, ИНН, дата рождения, место регистрации), данные доступа к аккаунтам (пароли и логины, ответы на секретные вопросы). Хотя жертва фишинга «сама» переходит по вредоносным ссылкам, и «сама» вводит персональные данные на фишинговых электронных ресурсах, она делает это под влиянием обмана. В основе своей обманутый пользователь считает, что передает данные легитимному сервису (банку, магазину, государственному portalу), и не дает согласия на передачу персональных данных третьему лицу (в данном случае – мошеннику). Таким образом, сбор информации происходит без законного согласия пользователя, что нарушает Конституцию Российской Федерации.

Фишинговые атаки в основном происходят, когда пользователь переходит по небезопасным сообщениям или письмам на электронной почте. Данные ссылки могут перенаправлять человека на поддельную торговую площадку, где при вводе данных для оплаты получается доступ к счетам жертвы. Для всех фишинговых атак характерно, что мошенники стремятся получить любую конфиденциальную информацию, которую в последующем могут использовать для собственной выгоды. Виды данных, которые могут быть украдены, очень разнообразный и зависят от того, на какую целевую аудиторию нацелена атака, или под какой предлог маскируются мошенники.

Данные, которые могут стать целью мошенников: учетные данные от электронной почты, социальных сетей, платежных сервисов, интернет-магазинов, облачных хранилищ; данные банковских карт; персональные данные пользователя; рабочие и корпоративные данные. Все это нарушает конституционные права и свободы человека и гражданина.

Основной целью киберпреступности является получение от жертвы денежных средств, либо конфиденциально информации, которую в последующем возможно использовать для извлечения выгоды. Как мы выяснили выше, в основном угрозе подвержены средства, хранящиеся на счетах в онлайн банках. Данные действия могут угрожать правам граждан на частную собственность, свободе распоряжаться данным имуществом. Такое право гарантируется статьей 35 Конституции Российской Федерации.

Фишинговые атаки могут быть нацелены как на похищение персональных данных у большого количества людей посредством атак на серверные центры и центры хранения защищенных данных, так и у отдельных людей.

Нередко такого вида кибератаки нацелены на похищение конфиденциальной информации, защищаемой Конституцией Российской Федерации, у конкретного человека, имеющего доступ к ключевой информации, позволяющей достичь поставленных целей. В основном фишинговые атаки проводятся посредством отправки SMS, либо электронных писем с ссылками, которые загружают на память

устройства вредоносный код, либо перенаправляют пользователя на электронные ресурсы, предназначенный для кражи данных, защищаемых Конституцией Российской Федерации.

Таким образом, фишинг по совокупности нарушает положения статьи 2 Конституции Российской Федерации. Положения данной статьи являются основополагающими к пониманию того, что именно нарушает данное киберпреступление. Фишинг посягает на высшие ценности - права и свободы человека (неприкосновенность частной жизни, право на собственность, в частности). Государство обязано защищать граждан от такого вида посягательств, в том числе путем создания законодательных актов, предусматривающих ответственность за фишинг и соответствующее возмещение ущерба.

Нарушение прав, гарантированных статьями 23, 24, 35 Конституции Российской Федерации, является нарушением тех основных положений, гарантированных статьей 2 Конституции Российской Федерации.

Для защиты конфиденциальных данных от нежелательного посягательства рекомендуется установить двухфакторную аутентификацию на все важные ресурсы, антивирус для обнаруживания вредоносных файлов и фишинговых ссылок. Также один из важных советов для защиты своих данных будет предостережение от перехода по подозрительным ссылкам из SMS и электронных писем.

Основными способами защиты от фишинговых атак, как от любого вида киберугроз, является внимательность и предусмотрительность к подозрительным рассылкам и электронным ресурсам.

Таким образом, в данной статье мы разобрали основные конституционные нормы, обеспечивающие права человека на неприкосновенность конфиденциальных данных, основные способы фишинговых атак и способы защиты от данного вида угроз.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // Собрание законодательства Российской Федерации, 01.07.2020, № 31; статьи 23, 24, 29, 35.
2. Фаина Ю. П. Уголовно-правовая характеристика мошенничества в сети Интернет // Вестник Югорского государственного университета. 2017. № 1-2 (44). С. 118.
3. Мочалов А. Н. Право на доступ в интернет: юридическое содержание и механизм реализации // Антиномии. 2021. № 4. С. 135–163.
4. Драчев, Я.В., Чеснокова А.А. Фишинг в практике известных компаний // Современные информационные технологии и информационная безопасность: сборник научных статей 3-й Всероссийской научно-технической конференции (2 февраля 2024 года). — Курск: ЗАО «Университетская книга», 2024. — С. 46-50.

*Малашкевич С. А.¹,
магистрант программы
Московского городского
педагогического университета*

*Научный руководитель:
Константинов А. В.,
доцент Департамента образовательных программ
Московского городского педагогического университета,
кандидат юридических наук, доцент*

ВЛИЯНИЕ МЕССЕНДЖЕРОВ НА ДИВЕРСИОННУЮ ДЕЯТЕЛЬНОСТЬ НЕСОВЕРШЕННОЛЕТНИХ, МЕТОДЫ ПРОФИЛАКТИКИ

В последние годы наблюдается рост случаев использования мессенджеров несовершеннолетними для участия в диверсионной и противоправной деятельности, что становится серьезной угрозой для общественной безопасности. Целью статьи является анализ влияния мессенджеров на участие несовершеннолетних в диверсионной деятельности и предложение методов профилактики таких явлений. В статье рассматриваются особенности использования мессенджеров для организации и координации действий подростков. Результаты подчеркивают важность комплексного подхода, включая правовое регулирование, образование и сотрудничество с общественными организациями. Материалы статьи полезны для специалистов в области социальной работы, правоохранительных органов и образовательных учреждений, служа основой для разработки рекомендаций по минимизации рисков, связанных с использованием мессенджеров в деструктивных целях.

Актуальность проблемы подростковой преступности в современной России продолжает оставаться высокой. Согласно данным ГИАЦ МВД России, в 2020 г. было зафиксировано 37 771 преступление, совершенное несовершеннолетними или при их соучастии, что составило 3,7 % от общего числа преступлений, в 2021 г. – 31 865 (3,1 %), в 2022 г. – 26 305 (2,9 %), а в 2023 г. – 27 325 (2,7 %) [1]. Несмотря на тенденцию к снижению числа преступлений, участие подростков в противоправной деятельности, включая преступления, совершаемые с использованием цифровых технологий, продолжает вызывать беспокойство. Одной из наиболее актуальных проблем является диверсионная деятельность, организуемая несовершеннолетними, которая представляет собой особую угрозу для национальной безопасности и стабильности общества. Использование современных технологий, включая мессенджеры, становится важным инструментом для координации таких действий, что усиливает необходимость разработки методов профилактики и правового регулирования.

¹ © Малашкевич С. А., 2025.

Использование мессенджеров, таких как Telegram, в контексте привлечения несовершеннолетних к диверсионной деятельности представляет собой значимую проблему для обеспечения безопасности и правопорядка. По данным Следственного Комитета России, лица, занимающиеся организацией диверсионных актов на территории РФ, активно используют платформы для связи с подростками, предлагая им участие в незаконных действиях [2]. Чаще всего привлечение осуществляется через мессенджер Telegram, где злоумышленники обещают несовершеннолетним денежное вознаграждение, которое, как правило, составляет от 10 до 15 тыс. рублей. Несовершеннолетние, в свою очередь, часто воспринимают такие предложения, как безобидные, не осознавая всей серьезности и опасности своих действий. Для них участие в этих актах порой становится чем-то вроде игры или квеста, а материальная выгода также может стать ключевым мотивом. В ряде случаев подростки идут на преступление из-за желания быстро заработать, не понимая общественной и юридической ответственности за свои поступки. Отсутствие жизненного опыта и недооценка возможных последствий для таких детей часто становятся причиной вовлечения в противоправную деятельность, что в свою очередь усиливает угрозу для безопасности общества.

Мессенджеры, как элементы цифровых коммуникационных технологий, играют ключевую роль в организации и координации действий подростков, особенно в контексте противоправной деятельности, такой как диверсионные акты. Как отмечает Е. А. Грецких, использование мессенджеров предоставляет уникальные возможности для общения, обмена информацией и планирования действий с минимальными рисками для пользователей, что делает их привлекательными для организаторов преступлений [3]. Мессенджеры обеспечивают высокий уровень анонимности и защищенности, что позволяет преступным группировкам и индивидуальным злоумышленникам эффективно манипулировать несовершеннолетними, не раскрывая своих личных данных. По результатам А. Ю. Головина, А. Р. Акиева и Е. В. Головиной, это особенно актуально для подростков, не имеющих достаточного опыта в интернет-безопасности и не осознающих полной угрозы со стороны виртуальных манипуляций [4]. В связи с этим, используя мессенджеры, преступники могут устанавливать контакты с подростками, не создавая явных подозрений у их окружения, что в значительной степени снижает вероятность выявления преступной деятельности.

В процессе координации действий через мессенджеры подростки получают инструкции, делятся сведениями о месте и времени исполнения задуманного преступления, а также получают, как правило, минимальные финансовые вознаграждения, что является дополнительным мотиватором для их участия. Сообщения могут передаваться в виде текстов, голосовых или видеозаписей, что позволяет создавать иллюзию безличности взаимодействия и снижать психологическое сопротивление у подростков. Как подмечает А. А. Чебуренков, одной из ключевых особенностей такого взаимодействия является отсутствие физического контакта, что в свою очередь упрощает использование мессенджеров для манипуляций с подростками [5]. Привлечение к противоправной деятельности часто происходит через различные формы лести или шантажа, что снижает кри-

тичность восприятия подростками происходящего, превращая это в некое игровое или экспериментальное занятие. По данным С. И. Глазырина, использование мессенджеров позволяет злоумышленникам быстро оценить ситуацию и при необходимости внести корректировки в планы, что повышает гибкость и эффективность действий [6]. Это также создает определенные сложности для правоохранительных органов, затрудняя отслеживание преступных связей и определение конкретных исполнителей.

Подобные особенности делают мессенджеры идеальными инструментами для подростков, вовлеченных в диверсионную деятельность, и усугубляют проблему криминализации молодежи в условиях цифровизации. В 2025 г., когда цифровые технологии продолжают стремительно развиваться и интегрироваться в повседневную жизнь, проблема вовлечения несовершеннолетних в преступную деятельность через мессенджеры становится все более актуальной. Для решения сложившихся проблем предлагаются следующие методы профилактики (табл. 1).

Таблица 1.

**Методы профилактики влияния мессенджеров
на диверсионную деятельность несовершеннолетних**

№	Метод профилактики	Описание
1	Повышение цифровой грамотности подростков	Осуществление образовательных программ и тренингов для формирования навыков безопасного использования мессенджеров и осознания рисков
2	Разработка и внедрение систем мониторинга и фильтрации контента в мессенджерах	Совместная работа правоохранительных органов, разработчиков и образовательных учреждений по созданию инструментов для отслеживания и блокировки противоправных действий
3	Психологическая поддержка и работа с подростками	Организация профилактических мероприятий с участием психологов, направленных на повышение осведомленности о последствиях вовлечения в преступную деятельность.
4	Укрепление взаимодействия между семьей, школой и правоохранительными органами	Создание системы быстрого реагирования и обмена информацией между семьями, образовательными учреждениями и правоохранительными органами для предотвращения вовлечения подростков
5	Криминализация действий по вовлечению несовершеннолетних в преступную деятельность через мессенджеры	Законодательные инициативы для усиления наказания за организацию преступной деятельности с участием несовершеннолетних через цифровые платформы

Продолжение таблицы 1.

6	Развитие социальной ответственности среди молодежи	Поддержка молодежных инициатив, направленных на помощь сверстникам, вовлеченным в опасную деятельность, создание платформ для безопасного обмена информацией и получения помощи

Предложенные методы профилактики являются частью необходимого комплексного подхода, направленного на уменьшение рисков вовлечения подростков в диверсионную деятельность и другие формы преступности через мессенджеры. Эти меры будут способствовать созданию более безопасного и защищенного цифрового пространства для молодежи, что позволяет не только предотвратить вовлечение подростков в противоправные действия, но и повысить уровень их осведомленности о потенциальных опасностях в сети. Важно подчеркнуть, что эффективное решение данной проблемы также требует синергии усилий со стороны государственных органов, образовательных учреждений и семей, а также активного участия общества в воспитании подростков в условиях цифровой эпохи.

Список литературы

1. Милованова М. М. Особенности установления обстоятельств, подлежащих доказыванию в процессе расследования диверсий на железнодорожных объектах, совершенных несовершеннолетними // Правовое государство: теория и практика. 2024. № 2 (76). С. 60–67.
2. СК назвал сумму, которую обычно обещают российским подросткам за диверсии. Электронный ресурс. Режим доступа: <https://tass.ru/obschestvo/19728575> (дата обращения: 18.02.2025 г.).
3. Грецких Е. А. Вовлечение несовершеннолетнего в совершение преступления: некоторые вопросы квалификации // Актуальные проблемы российского права и законодательства: Сборник материалов XVI Всероссийской научно-практической конференции, Красноярск. 2023. С. 179–182.
4. Головин А. Ю., Акиев А. Р., Головина Е. В. Дистанционное вовлечение несовершеннолетних в преступную деятельность как объект криминалистического исследования // Правовое государство: теория и практика. 2024. № 2 (76). С. 24–30.
5. Чебуренков А. А. Криминалистические проблемы установления негативного влияния взрослых на несовершеннолетних с целью вовлечения их в совершение преступлений // Правовое государство: теория и практика. 2024. № 2 (76). С. 103–114.
6. Глазырин С. И. Преступления диверсионной направленности: новый подход в области обеспечения экономической безопасности и обороноспособности российской федерации на современном этапе // Правопорядок: история, теория, практика. 2024. № 1 (40). С. 167–171.
7. Константинов А. В. Особенности осуществления деятельности подразделений по делам несовершеннолетних в условиях режима самоизоляции / А. В. Константинов // Портрет инспектора по делам несовершеннолетних : сборник

научных трудов Всероссийской конференции, Москва, 28 мая 2020 года. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2020. – С. 239-240. – EDN ZWWZIR.

Собаценок И. А.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я Кикотя*

Научный руководитель:

Поликарпова Е. В.,

*старший преподаватель
кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя*

ДАРКНЕТ КАК СОВРЕМЕННАЯ АНОНИМНАЯ СРЕДА: ПРОБЛЕМЫ ПРАВОПОРЯДКА И СПОСОБЫ БОРЬБЫ С НЕЗАКОННОЙ ДЕЯТЕЛЬНОСТЬЮ

Даркнет (англ. darknet – «темный интернет») представляет собой часть интернета, которая не индексируется поисковыми системами и доступна только через специальные анонимные сети, такие как Tor, I2P и другие. Эта сеть используется как для обеспечения конфиденциальности пользователей, так и для незаконных операций, включая торговлю наркотиками, оружием, фальшивыми документами и другими запрещенными товарами. В последние десятилетия даркнет привлекает внимание не только пользователей, но и правоохранительных органов, поскольку является средой, где анонимность способствует росту киберпреступности.

В условиях глобализации и развития информационных технологий даркнет становится не только ареалом для нелегальной деятельности, но и проблемой для правоохранительных органов всего мира, в том числе России. Научные исследования, проводимые в различных странах, показывают, что с каждым годом количество преступлений, совершаемых через даркнет, растет, и это затрудняет их раскрытие. В частности, в России увеличивается количество преступлений, связанных с наркотиками, кибермошенничеством и торговлей фальшивыми документами через даркнет. Основной целью данной статьи является комплексный анализ проблем правопорядка, возникающих в связи с использованием даркнета, а также предложение путей решения этих проблем с учетом существующих правовых и технических средств.

Даркнет является подмножеством так называемого глубокого интернета (deep web), который включает в себя все ресурсы, не индексируемые традиционными поисковыми системами. В отличие от поверхностного интернета (clear web), доступного всем пользователям без ограничений, даркнет использует особые про-

¹ © Собаценок И. А., 2025.

токолы и программы для обеспечения анонимности. Одним из наиболее известных таких протоколов является Tor (The Onion Router), который позволяет скрывать IP-адреса пользователей и их действия в сети.

Даркнет не является монолитным и включает в себя различные сети и ресурсы. Помимо Tor, для анонимного серфинга часто используются сети I2P (Invisible Internet Project) и Freenet, каждая из которых имеет свои особенности и технологии обеспечения безопасности и конфиденциальности. Эти сети позволяют пользователям обмениваться данными, не опасаясь преследования со стороны правоохранительных органов.

Даркнет обладает рядом уникальных характеристик, которые отличают его от традиционных интернет-ресурсов. Прежде всего, это анонимность пользователей, которая достигается за счет многократного шифрования данных и маршрутизации трафика через несколько серверов. Эта особенность позволяет пользователям скрывать свое местоположение, что делает невозможным отслеживание их действий без специальных технических средств.

Кроме того, в даркнете используются криптовалюты, такие как биткойн и монеро, которые предоставляют дополнительные возможности для анонимных транзакций. Эти валюты позволяют проводить финансовые операции без использования традиционных банковских структур, что делает систему безопасной для пользователей, совершающих незаконные операции. Одним из наиболее распространенных видов преступлений, связанных с даркнетом, — это торговля наркотиками. На специализированных торговых площадках даркнета пользователи могут анонимно покупать и продавать различные запрещенные вещества, от марихуаны до тяжелых наркотиков, таких как метамфетамин и фентанил [1].

Исследования, проведенные в России и за рубежом, показывают, что количество наркотических сделок, совершаемых через даркнет, с каждым годом увеличивается. Это связано с тем, что даркнет предоставляет торговцам и покупателям анонимность, что делает их труднее обнаруживаемыми для правоохранительных органов. В частности, полиция часто сталкивается с проблемами, связанными с тем, что преступники используют криптовалюты для оплаты, что затрудняет финансовые расследования.

По данным Федеральной службы по контролю за наркотиками (ФСКН России), через даркнет за последний год было зафиксировано увеличение числа крупных каналов сбыта наркотиков. Важно отметить, что использование даркнета для торговли наркотиками не ограничивается только российским сегментом интернета — это глобальная проблема, затрагивающая многие страны мира.

Даркнет также используется для незаконной торговли оружием и фальшивыми документами. Торговцы оружием могут продавать как легкие огнестрельные оружия, так и более сложные боевые системы, включая автоматы и гранатометы. Кроме того, в даркнете часто приобретают поддельные паспорта, водительские удостоверения и другие документы, которые можно использовать для преступных целей.

Особую угрозу представляет тот факт, что торговля оружием и фальшивыми документами через даркнет может привести к созданию целых преступных се-

тей, осуществляющих деятельность на международном уровне. Проблема заключается в том, что эти сети могут использовать сложные схемы, которые затрудняют их выявление.

В даркнете также активно развиваются схемы кибермошенничества, включая продажу украденных данных кредитных карт, фишинг, а также услуги по взлому аккаунтов и компьютеров. Преступники, действующие через даркнет, продают не только персональные данные, но и программное обеспечение для кибератак [2].

Одной из значительных проблем является то, что при таком типе преступлений трудно установить точные масштабы ущерба. Кибермошенники могут действовать с использованием анонимных учетных записей и защищенных каналов связи, что затрудняет сбор доказательств и расследование таких дел.

Важной проблемой является отсутствие четкой правовой базы для борьбы с преступлениями, совершаемыми через даркнет. Несмотря на существование международных соглашений, таких как Конвенция о киберпреступности [3], эффективность их применения ограничена из-за анонимности даркнета и сложности в установлении юрисдикции.

В российском законодательстве существует ряд норм, которые регулируют борьбу с киберпреступностью, однако эти нормы недостаточны для полноценной борьбы с преступлениями в даркнете. Специфические действия, такие как использование криптовалют, не всегда находят свое отражение в российском законодательстве, что приводит к правовым пробелам. Для эффективной борьбы с преступностью в даркнете необходимо создать специализированную правовую базу, которая будет учитывать особенности анонимных сетей и использование криптовалют. Важно разработать механизмы для отслеживания незаконных финансовых транзакций, а также создать юридические нормы для пресечения использования анонимных сетей для совершения преступлений [4].

Так как даркнет является глобальной сетью, важно развивать международное сотрудничество между государствами. Это включает в себя обмен информацией между правоохранительными органами разных стран, совместные операции по выявлению и задержанию преступников, а также создание единой правовой базы для борьбы с преступностью в даркнете. Технические решения, такие как алгоритмы для анализа транзакций в криптовалютах и системы для мониторинга даркнета, являются важными инструментами в борьбе с преступностью. Использование искусственного интеллекта и машинного обучения для анализа поведения пользователей и выявления аномальных транзакций может значительно повысить эффективность расследований.

Кроме того, важно развивать программы профилактики, направленные на снижение привлекательности даркнета для пользователей. Это включает в себя как повышение осведомленности граждан о рисках, связанных с использованием даркнета, так и создание образовательных программ, направленных на развитие цифровой грамотности.

Даркнет представляет собой как угрозу, так и возможность для общества. С одной стороны, он является местом для защиты конфиденциальности и свободы слова, с другой – способствует распространению незаконной деятельности. В

связи с этим необходимо разработать комплекс мер для борьбы с преступной деятельностью в даркнете, включая улучшение законодательства, международное сотрудничество и развитие новых технологий. Важно отметить, что борьба с даркнет-преступностью должна быть сбалансированной и учитывать, как угрозы, так и возможности, которые даркнет предоставляет для защиты прав и свобод граждан.

Список литературы

1. Соколова Е. В. Киберпреступность в России: современные угрозы и способы борьбы / Е. В. Соколова. – М.: Юрайт, 2022.
2. Журавлев А. Н. Технологии анонимности: даркнет и его влияние на правопорядок / А. Н. Журавлев. – СПб.: Лань, 2021.
3. Петров И. В. Правовые аспекты борьбы с киберпреступностью в даркнете / И. В. Петров. – М.: Норма, 2023.
4. Иванова М. С. Торговля наркотиками в даркнете: правовые и социальные проблемы / М. С. Иванова. – М.: Российская академия наук, 2022.
5. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационнокоммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года.
6. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.
7. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Солодова Ю. С.¹,
 слушатель института подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Константинов А. В.,
 заместитель начальника кафедры противодействия преступлениям
 в сфере информационно-телекоммуникационных технологий
 Московского университета МВД России имени В.Я. Кикотя,
 кандидат юридических наук, доцент

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБНАРУЖЕНИИ И РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ: ОТЕЧЕСТВЕННЫЙ И ЗАРУБЕЖНЫЙ ОПЫТ

Высокие темпы цифровизации, развитие технологий и внедрение искусственного интеллекта во все сферы жизни человека в последние десятилетия, привели к увеличению числа киберпреступлений и росту киберугроз, посягающих не только на безопасность физических и юридических лиц, но и государства в целом. Вопросы защиты от кибератак и расследование преступлений в сфере информационных технологий в современных реалиях становятся все более актуальными. Одним из перспективных направлений в данной области является использование искусственного интеллекта для обнаружения и расследования киберпреступлений.

В нормативных правовых актах Российской Федерации нет закрепленного понятия «киберпреступность». В современной юридической науке под киберпреступлениями понимаются преступления, связанные с компьютерными технологиями и информационным пространством, направленные на имущество, персональные данные, жизнь, здоровье и иные виды ущерба гражданам и государству. Данный вопрос является особо актуальным, многие ученые и исследователи предпринимают попытку дать полное определение данному понятию. Так, по мнению Д. Н. Карпова киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба, индивиду, организации или государству посредством любого технического средства с доступом в Интернет [1, с. 46–50]. По нашему мнению, данное понятие является наиболее удачным, так как раскрывает всю сущность рассматриваемого нами феномена.

Искусственный интеллект – разноплановое явление, в отношении правоохранительной деятельности, так как воздействует в двух вариациях:

1. Как инструмент, способствующий совершению противоправных деяний.

¹ © Солодова Ю. С., 2025.

2. Как инструмент, защищающий от таких угроз.

Так, искусственный интеллект может быть использован для анализа больших объемов данных, выявления различных закономерностей и аномалий, которые могут указывать на наличие преступной деятельности в киберпространстве. Рассмотрим каждый из направлений данной деятельности подробно:

1. Обнаружение аномалий происходит посредством анализа действий пользователей и серверов в сети Интернет и выявления подозрительных активностей на них. Алгоритмы отслеживают отклонения от нормального функционирования и сразу оповещает об угрозе, к таким можно отнести попытки взломов аккаунта, ложные транзакции, попытки несанкционированного доступа к информации.

2. Программы искусственного интеллекта настраиваются на распознавание характерных признаков отдельных видов киберпреступлений и анализирует поведение лиц в сети Интернет, с помощью полученной информации, происходит проверка действий на предмет скрытых угроз, предупреждая о ней.

3. Помимо сообщения об угрозе, искусственный интеллект может предсказывать их, используя исторические данные, изучая алгоритмы, а также информацию, находящуюся на различных серверах хакеров или сведения, оставленные ими в социальных сетях.

4. Искусственный интеллект также может упрощать работу, связанную с поиском «цифровых следов», так, например, программы искусственного интеллекта могут анализировать сайты и составлять журналы активности отдельных пользователей на сайтах с хакерской и прочей тематикой.

Но несмотря на все положительные аспекты, лица, имеющие преступный умысел, могут использовать его в своих целях. Так, в Российской Федерации одними из наиболее часто встречаемых киберпреступлений являются:

1. Хакерские атаки на частные и государственные информационные системы.
2. Распространение вредоносных программ.
3. Кража персональных данных.
4. Фишинговые атаки, направленные на получение конфиденциальной информации граждан и организации.
5. Различные мошеннические действия в сфере высоких технологий, в том числе с использованием поддельных сайтов, платежных систем, QR-кодов и прочего.

Оценка зарубежной практики борьбы с киберпреступностью, показывает, что чаще встречаются следующие виды данных преступлений:

1. Кибератаки на критически важные объекты инфраструктуры, к которым относятся энергетические системы, узлы связи, военные базы и прочее.
2. Использование вредоносного программного обеспечения для кражи интеллектуальной собственности.
3. Мошенничество в сфере финансов, включая схемы с фальсификацией банковских карт.
4. Создание онлайн-платформ для незаконного оборота наркотиков, оружия и других запрещенных товаров.
5. Распространение детской порнографии; и прочее.

Анализ отечественного и зарубежного опыта борьбы с киберпреступностью

позволяет выявить тенденции развития рассматриваемого нами негативного явления, что способствует созданию методик, способствующих разработать подходы к противодействию, определить стратегии в борьбе с выделенными видами киберпреступлений.

На современном этапе развития общества искусственный интеллект постепенно вводится в деятельность сотрудников полиции разных стран. Так, например, одним из самых распространенных направлений деятельности искусственного интеллекта является распознавание лиц, в том числе используемое и на территории Российской Федерации. Только в Москве видеонаблюдение со встроенными программами искусственного интеллекта способствует раскрытию 70 % преступлений. Одной из разработок в данной сфере является технология NtechLa, позволяющая распознавать лица и силуэты людей, она позволяет разыскивать лиц, подозреваемых в совершении противоправных деяний, а также решать вопросы некриминального характера, например, управлять пассажиропотоком.

Анализируя опыт зарубежных правоохранительных органов, стоит отметить использование искусственного интеллекта национальной полицией Голландии. Нейросети, подключаемые к работе сотрудников правоохранительных органов, классифицируют и готовят уголовные дела к расследованию, с помощью изучения и анализа предоставленных документов и вещественных доказательств.

Перспективы развития борьбы с преступностью в киберпространстве, связаны с совершенствованием законодательства, международным сотрудничеством, так как данные преступления чаще всего носят транснациональный характер, повышением квалификации специалистов данной сферы и развитием технологий в целом.

Потенциал искусственного интеллекта в борьбе с киберпреступностью, по нашему мнению, колоссален, ведь данные технологии обладают значительными возможностями для анализа больших объемов данных, выявлению закономерностей и аномалий. Однако для глобального внедрения искусственного интеллекта в правоохранительную деятельность, необходимо решить ряд правовых, технических организационных вопросов.

Таким образом, искусственный интеллект представляет собой мощный инструмент в борьбе с киберпреступностью, который способен значительно повысить эффективность обнаружения и расследования преступлений, совершаемых в киберпространстве. Однако для достижения максимальных результатов, необходимо учитывать, как потенциал, способный значительно упростить работу правоохранительных органов, так и ограничения технологий искусственного интеллекта, а также ряд рисков.

Список литературы

1. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 46–50. – Библиогр.: с. 50.

2. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

3. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Соломина А. А.¹,
*курсант института подготовки сотрудников
для органов предварительного
расследования Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Константинов А. В.,
*заместитель начальника кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ИНСТИТУЦИОНАЛЬНЫЕ МЕХАНИЗМЫ ПРИЗНАНИЯ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В РОССИИ: ЭКСПЕРТНЫЕ ПРАКТИКИ МВД РОССИИ И ФСБ РОССИИ

В российской правовой системе процедура признания организаций и физических лиц террористическими представляет собой сложный административно-судебный процесс с выраженной ведомственной составляющей. Несмотря на формальное закрепление данной прерогативы за судебными органами, фактически ключевая роль в формировании доказательной базы принадлежит экспертным структурам силовых ведомств, что вызывает серьезные дискуссии о соблюдении баланса между интересами государственной безопасности и защитой гражданских свобод.

Правовую основу данного процесса составляет Федеральный закон № 35-ФЗ «О противодействии терроризму», содержащий расплывчатое определение террористической деятельности как «идеологически мотивированного насилия или угрозы его применения». Нормативная неопределенность этой дефиниции создает предпосылки для расширительного толкования, что подтверждается анализом правоприменительной практики последнего десятилетия.

Институциональная структура противодействия терроризму включает специализированные подразделения ФСБ России (Научно-исследовательский центр и Управление "А") и МВД России (ГУПЭ и экспертно-криминалистические центры). Эти структуры обладают широкими полномочиями по проведению экспертиз, однако их методики и критерии оценки остаются закрытыми для общественного контроля, что порождает серьезные сомнения в объективности принимаемых решений. [2, с. 211].

Анализ судебной практики выявляет устойчивую тенденцию к расширительной интерпретации понятия терроризма. С 2013 г. в России было запрещено более 50 организаций, включая не только классические террористические группировки, но и религиозные объединения с исключительно мирной деятельностью,

¹ © Соломина А. А., 2025.

такие как «Свидетели Корана». Особую озабоченность вызывает практика признания террористическими оппозиционных движений на основании их публичных высказываний, как это произошло в 2023 г. с «Армией воли народа».

Показательным примером системных проблем стало дело «Сети» (2019 г.), где группа молодых анархистов была осуждена за создание «террористического сообщества» на основании их частной переписки и спорных экспертных заключений. Этот случай наглядно продемонстрировал, как отсутствие четких критериев и закрытый характер экспертных методик могут привести к уголовному преследованию за мысли и разговоры, не подкрепленные конкретными действиями [1].

Критический анализ существующей системы позволяет выделить три ключевые проблемы: политизацию понятия «терроризм», отсутствие механизмов независимой проверки экспертных заключений и размытость юридических формулировок в законодательстве. Последнее особенно наглядно проявляется в случаях квалификации как экстремистских цитат из литературных произведений или репостов в социальных сетях.

Первая и наиболее существенная проблема заключается в прогрессирующей политизации понятия «терроризм», когда под это определение подводятся различные формы политического инакомыслия. На практике это приводит к парадоксальным ситуациям, когда участники мирных акций или авторы критических публикаций приравниваются к террористам. Ярким примером может служить дело 2022 г., в котором оппозиционный политик был привлечен к ответственности за высказывания, не содержавшие призывов к насилию, но критиковавшие действующую власть. Статистический анализ судебных решений последних лет показывает, что около трети обвиняемых по «террористическим» статьям фактически занимались легальной политической деятельностью.

Вторая системная проблема связана с отсутствием действенных механизмов независимой проверки экспертных заключений. Современная практика демонстрирует тревожную ведомственную замкнутость: подавляющее большинство экспертиз (по некоторым оценкам – до 89%) проводятся исключительно сотрудниками ФСБ России и МВД России без привлечения независимых специалистов. Особую озабоченность вызывает непрозрачность применяемых методик – лишь 12 % из них имеют должное научное обоснование, остальные разработаны внутри ведомств и не подвергались внешней экспертной оценке. Судебная практика показывает, что в 97 % случаев суды отказываются рассматривать альтернативные экспертные заключения, представленные защитой. Ситуацию усугубляет кадровый вопрос: только четверть привлекаемых экспертов обладает профильным образованием в области лингвистики или политологии, что ставит под сомнение качество проводимых исследований.

Третья ключевая проблема – крайняя размытость юридических формулировок в действующем законодательстве. Федеральный закон «О противодействии терроризму» содержит настолько широкие и неконкретные определения, что допускает диаметрально противоположные трактовки одних и тех же понятий. Отсутствие четких критериев отнесения материалов к экстремистским приводит к

абсурдным правоприменительным решениям. В судебной практике зафиксированы случаи признания экстремистскими цитат из классической литературы (дело о стихах Мандельштама, 2021 г.), исторических документов (дело о репосте Всеобщей декларации прав человека, 2022 г.), научных работ по политологии (дело о диссертации по истории анархизма, 2023 г.). Особую тревогу вызывает несоответствие российского законодательства международным стандартам в части разграничения между призывами к насилию и мирной критикой власти, что неоднократно отмечалось в решениях ЕСПЧ.

Современная судебная практика изобилует показательными примерами, иллюстрирующими эти системные проблемы. Московский городской суд в 2023 г. признал экстремистскими материалы, содержащие цитаты из Льва Толстого о непотворении злу насилием, мотивируя это решение «пропагандой идеологии, противоречащей государственной политике». Верховный Суд РФ в 2024 г. поддержал запрет молодежного объединения за публикацию аналитической статьи о социальном неравенстве, которую эксперты ФСБ России квалифицировали как «пропаганду террористических методов». Конституционный Суд в том же году признал законным привлечение к ответственности за простой репост новости о деятельности запрещенной организации без каких-либо комментариев со стороны пользователя.

Сравнительный анализ международного опыта (Германия, Канада, Швеция) демонстрирует альтернативные подходы к решению аналогичных задач, включая обязательное участие независимых экспертов, многоуровневую систему проверки и публичное обсуждение вопросов запрета организаций. Эти практики заслуживают внимательного изучения и возможной адаптации к российским условиям.

Сложившаяся ситуация требует комплексного реформирования существующей системы. В первую очередь необходимо законодательное закрепление четких и недвусмысленных критериев террористической деятельности, исключающих субъективное толкование. Во-вторых, следует ввести институт альтернативных экспертиз с участием независимых специалистов из научного сообщества. В-третьих, важно обеспечить реальную возможность обжалования решений экспертных комиссий, включая обращение в международные инстанции [3, с. 10].

Без этих изменений институт признания организаций террористическими рискует трансформироваться из инструмента обеспечения безопасности в механизм ограничения гражданских свобод, что в конечном итоге может подорвать доверие ко всей системе противодействия терроризму. Особую актуальность приобретает поиск разумного баланса между необходимостью защиты национальной безопасности и соблюдением фундаментальных прав и свобод граждан, что должно стать предметом дальнейших междисциплинарных исследований.

Список литературы

1. ВЕСТИ. Дело «Сети»: новые данные. URL: <https://www.vesti.ru/article/1398100>.

2. Вострокнутов А. Л., Зыков В. В. Организация межведомственного взаимодействия правоохранительных органов в противодействии преступлениям террористического характера // Вестник экономической безопасности. 2019. № 4.

3. Савинский А. В. о повышении эффективности уголовно-правового противодействия терроризму // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1 (35).

4. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

5. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Суровикин А. Д.¹,
*курсант института
подготовки сотрудников для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Токолов А. В.,
*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ

Сегодня невозможно представить жизнь без информационно-телекоммуникационных технологий. Мобильные телефоны, компьютеры, информационно-телекоммуникационная сеть Интернет – постоянные спутники современного человека на протяжении целого дня. Информационные технологии в значительной степени трансформируют все бесчисленное множество общественных отношений. Предоставление государственных услуг осуществляется через интернет порталы, просмотр расписания общественного транспорта уходит в сеть, появление сервисов доставки продуктов питания и маркетплейсов, развитие дистанционного банкинга, не говоря уже о всевозможных мессенджерах, социальных сетях, онлайн платформах для просмотра видео. Все это и многое другое так или иначе влияет на общество.

Помимо этого, современные технологии активно применяются в правоохранительной деятельности. Так, информационные системы автоматической регистрации сценариев индексирования видеоинформации (ПАРСИВ), СПО «Паутина», АПК «Безопасный город», ГАИС «Сфера», ПТК «Розыск-Магистраль» и иные оказывают незаменимую помощь полиции и иным правоохранительным органам в предупреждении уличной преступности, раскрытии и расследовании противоправных деяний, розыске преступников и без вести пропавших лиц. Эффективность этих информационных систем подтверждается статистикой, собранной ФКУ «ГИАЦ МВД России», согласно которой ежегодно уменьшается количество зарегистрированных преступлений, совершенных в общественных местах. Появляются оперативно-розыскные мероприятия, связанные с применением информационных технологий, такие как получение компьютерной информации.

В системе МВД России появляются подразделения, деятельность которых направлена на предупреждение, пресечение, раскрытие, расследования преступлений в сфере информационно-коммуникационных технологий (далее – ИТТ),

¹ © Суровикин А. Д., 2025.

выработке и реализации государственной политики, нормативному правовому регулированию в области совершенствования информационных и телекоммуникационных технологий, автоматизированных информационных систем, систем и средств связи. К ним относятся такие как Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК), Бюро специальных технических мероприятий (БСТМ), Управление по расследованию организованной преступной деятельности в сфере незаконного оборота наркотических средств и информационно-коммуникационных технологий Следственного Департамента МВД России, Департамент информационных технологий, средств связи и защиты информации (ДИТСИЗИ) [1].

Однако, вместе с этим происходит и трансформация преступности. Ежегодно наблюдается рост преступлений, совершенных с использованием ИТТ. Так, в январе–декабре 2024 г. доля таких преступлений составила 40 % от общего числа [2], то есть приблизительно 764 тыс. преступлений, а ущерб, причиненный ими, превысил 200 миллиардов рублей. Прирост количества информационных преступлений составил 13,1 % по сравнению за аналогичный период 2023 г., что, несомненно, говорит о важности развития мер борьбы с преступлениями такого характера.

Президент Российской Федерации на расширенном заседании Коллегии МВД России заявил о важности поиска новых мер реагирования на угрозы, которые ставят перед обществом и государством киберпреступники. В связи с этим, в качестве одной из первостепенных задач МВД России Верховным Главнокомандующим была поставлена задача «во взаимодействии с другими профильными ведомствами – искать новые, более эффективные методы борьбы с этой угрозой, в том числе в рамках единой системы противодействия подобным преступлениям» [3].

Киберпреступность не однородна и внутри нее также происходят изменения. Для выявления этих изменений нами был взят самый актуальный на сегодняшний день сборник «Состояние Преступности В России» Главного информационно-аналитического центра МВД России за январь–март 2025 г. и сравнен со сборником за аналогичный период 2024 г. В анализе будет учитываться объем, структура и территория распространения преступности в сфере ИТТ, а также раскрываемость этих преступлений.

Всего за первые 3 месяца 2025 г. было зарегистрировано 184 632 преступления в сфере компьютерной информации, в то время как за январь – март 2024 г. – это число составило 179 228. Прирост составил 5 404 противоправных деяния или 3 %. Увеличилось и количество тяжких и особо тяжких преступлений – с 85 168 до 95 681, то есть на 10 513 или на 10,9 %. При этом вырос и показатель раскрываемости, который достиг отметки в 55 507 преступлений или 30 % от общего числа против 47 242 или 26 %. Соотношение раскрытых и нераскрытых преступлений все еще не удовлетворяет потребностям общества и государства от преступных посягательств в сфере ИТТ, однако, наличие положительной динамики свидетельствует об эффективности деятельности подразделений УБК и других служб МВД России.

Удивительно, но в анализируемом отчетном периоде наблюдается значительный спад количества традиционных для киберпреступности деяний против собственности. В совокупности кражи (ст. 158 УК РФ) и мошенничества (ст.ст. 159, 159.3 и 159.6 УК РФ) образуют число 111 152, что составляет 60,2 % от всех преступлений в сфере ИТТ, в то время как в прошлом году эти показатели составляли 115 833 и 64,6 % соответственно. Если в 2024 г. было зарегистрировано 26 075 краж, то в 2025 г. их количество сократилось до 22 620, то есть спад составил 13,3 %, в то время как общее количество краж уменьшилось всего на 1,8 %. Также спад наблюдается по всем видам мошенничества – традиционное или простое мошенничество на 1,4 %, мошенничество с использованием электронных средств платежа на рекордные 92,7 % (с 247 до 18), а мошенничество с использованием компьютерной информации на 75,8 % (со 149 до 36). При этом показатель раскрываемости таких преступлений вырос только по простым мошенничествам и составил 11 120 вместо 10 000 (прирост составил 8,5 %). Раскрываемость краж уменьшилась на 18,4 %, преступлений, предусмотренных ст. 159.3 УК РФ на 84,6 % (всего 4 преступления против 26 в предыдущем году), ст. 159.6 на 82,8 % (46 вместо 267).

Анализ этих показателей позволяет прийти к выводу:

1. Меры предупреждения имущественных преступлений в сфере ИТТ работают эффективно.

2. Преступники находят более сложные способы совершения преступлений, что затрудняет их раскрытие и дальнейшее расследование. Простые звонки из «службы безопасности банка» или «ФСБ» уже не работают так эффективно, как несколько лет назад, что толкает кибермошенников на поиски иных методов, в том числе технических, совершения преступлений.

Также сокращается и количество преступлений, связанных с незаконной организацией азартных игр (ст. 171.2 УК РФ) и изготовлением порнографических материалов, в том числе с использованием несовершеннолетних на 16,7 % и 0,2 % соответственно.

В связи с совершенным 22 марта 2024 г. терактом в «Крокус Сити Холле», регулярной террористической и диверсионной деятельностью, проводимой на территории Российской Федерации при непосредственном участии спецслужб Украины и Коллективного Запада, возросло количество преступлений, связанных с публичными призывами к осуществлению террористической деятельности, публичным оправданием терроризма или пропагандой терроризма (ст. 205.2 УК РФ). Количество таких преступлений увеличилось за отчетный период на 90,3 %.

Значительную долю в структуре преступлений в сфере ИТТ составляет незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконный сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ). Если в январе – марте 2024 г. наблюдался спад таких преступлений на 11,6 % и составлял 18 868 деяний, то в 2025 г. имеется заметный рост на 73,1 %. При этом из 32 653 преступлений раскрыты 20 136, то есть 61,7 %. Несмотря на это, хотя количество раскрытых преступлений увеличилось на 59,2 % с 12 650 до 20136

преступлений, соотношение раскрытых и зарегистрированных преступлений в 2024 г. было выше и составляло 67 %.

Что касается преступлений, предусмотренных главой 28 УК РФ (Преступления в сфере компьютерной информации), в 2025 г. их количество начало снижаться. Если в 2024 г. их количество увеличилось на 368,7 % и достигло 22 472 деяний, то сейчас наблюдается спад на 18,1 %. Так. Самое распространенных преступлений этой главы – неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – было зарегистрировано всего 18 340 вместо 22 472 (-18,1 %), а создания и распространения компьютерной вредоносных компьютерных программ выявлено на 10,6 % меньше – 59.

Территориальная распространенность преступлений в сфере ИТТ также претерпела значительные изменения. Так, наибольшие темпы прироста в 2025 г. наблюдаются в Чеченской Республике, Магаданской области и Республике Саха (Якутия), а наибольший удельный вес в общей структуре преступности отмечен в Республике Марий Эл, ХМАО–Югра и ЯНАО. Стоит отметить также, что в общей структуре преступности в Чеченской республике преступления в сфере ИТТ составляют всего 16,1 %, а по темпам прироста предварительного расследования по этим преступлениям она занимает первое место с приростом в 1080,0 %. Наибольшая раскрываемость наблюдается в Республике Дагестан (77,5 %), Костромской области (64,1 %) и Рязанской области (63,9 %). В 2024 г. наибольшая раскрываемость была в Тамбовской и Костромской областях (70,3 % и 65,3 %), а также республика Дагестан (59,7 %).

Таким образом, проанализировав актуальную статистику преступности в Российской Федерации, можно выявить следующие тенденции преступлений в сфере ИТТ:

1. Количество преступлений с этой области и число тяжких и особо тяжких из них растет и будет продолжать расти.
2. Меры по предупреждению и раскрытию преступлений эффективно работают, о чем свидетельствует снижение количества ряда преступлений и рост процента их раскрываемости.
3. Преступления против собственности становятся более сложными, что затрудняет их раскрытие имеющимися у органов внутренних дел силами и средствами.
4. Снижается количество преступлений против собственности, общественной нравственности, в сфере экономической деятельности, а также в сфере компьютерной информации.
5. Заметный рост наблюдается среди преступлений, связанных с оборотом некритических средств, психотропных веществ и их прекурсоров, а также преступлений против общественной безопасности.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) 13 июня 1996 года N 63-ФЗ // СПС «Консультант Плюс» URL:

https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 08.05.2025).

2. Указ Президента Российской Федерации «Вопросы Министерства внутренних дел Российской Федерации» от 01.03.2011 № 248 // Российская газета. – 2011 г. – № 43. – с изм. и допол. в ред. от 02.04.2025.

3. Состояние преступности в России за январь–декабрь 2024 года . – М.: ФКУ «Главный информационно-аналитический центр», 2025. – 64 с.

4. Состояние преступности в России за январь–март 2024 года . – М.: ФКУ «Главный информационно-аналитический центр», 2024. – 64 с.

5. Состояние преступности в России за январь–март 2025 года . – М.: ФКУ «Главный информационно-аналитический центр», 2025. – 64 с.

6. Расширенное заседание коллегии МВД // Официальные сетевые ресурсы Президента России. URL: <http://www.kremlin.ru/events/president/transcripts/76408> (дата обращения: 07.05.2025).

7. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

8. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Филонова Д. А.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Рудин А. В.,

*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

УГРОЗЫ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С РАЗВИТИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

В современном мире блокчейн-технология представляет собой значительный шаг вперед в области хранения информации. В эпоху растущей потребности в надежной и защищенной информации ее важность трудно переоценить. Многие эксперты полагают, что сфера ее применения практически безгранична. Она открывает новые горизонты в государственном секторе, финансовых институтах и производственной деятельности.

Что же такое блокчейн? Блокчейн – это децентрализованная система хранения данных, которая фиксирует все операции, совершаемые участниками сети. Данные хранятся в виде блоков, которые связаны между собой [1]. В каждом блоке содержится информация о нескольких транзакциях. В децентрализованной блокчейн-системе каждый пользователь, иницирующий новую операцию, присваивает ей временную метку, записывает данные и вносит в свой персональный электронный журнал. Затем все эти операции распространяются по всей сети между всеми ее участниками.

Согласно мнению Банка Англии, блокчейн представляет собой технологическое решение, позволяющее взаимодействовать и безопасно обмениваться информацией о событиях даже незнакомым сторонам [2].

Благодаря своей архитектуре, система блокчейн практически исключает возможность незаметной модификации данных, что делает ее весьма устойчивой к коррупционным рискам.

Для наглядности можно представить ее как цепь «chain», где каждый элемент – это «блок», содержащий информацию о транзакции или событии. Эта цепь обладает высокой степенью защиты от разрушения или изменения. Таким образом, блокчейн – это своего рода неподдельная цифровая летопись действий.

Именно благодаря высокой надежности и безопасности, блокчейн находит применение в оптимизации финансовых процессов, а также в обмене данными

¹ © Филонова Д. А., 2025.

между физическими лицами, коммерческими организациями и государственными учреждениями.

Концепция блокчейна не связана с какой-либо конкретной страной, представляя собой компонент всемирной сети. Его возникновение датируется 2008 г., когда неизвестный автор или группа лиц, известных под именем Сатоши Накамото, представили научную работу, ставшую основополагающим документом для этой революционной технологии. В этой работе были изложены ключевые принципы и потенциал разработки децентрализованной системы проведения финансовых операций.

За прошедшее время возникло множество гипотез относительно истинного автора этой публикации. Существуют весомые аргументы в пользу того, что автором был человек, говорящий на русском языке. Изначальный блок был сгенерирован в 2009 г., и на сегодняшний день в мире насчитывается более 2000 разнообразных криптовалютных активов, основанных на различных вариациях блокчейна.

Термины «блокчейн», «криптовалюта» и «биткоин» нередко вызывают путаницу, их даже ошибочно считают взаимозаменяемыми. Попробуем внести ясность и понять, чем они отличаются друг от друга.

Первопроходцем в мире цифровых валют является Биткоин, наиболее узнаваемый представитель криптографии, функционирующий на базе блокчейн-технологии. Суть его работы заключается в перемещении активов между электронными кошельками пользователей. Прозрачность системы позволяет каждому участнику отслеживать историю всех операций, зарегистрированных в блокчейне с момента его запуска в 2009 г.

Именно Биткоин, как первая криптовалюта, внедрившая блокчейн, послужил катализатором глобального интереса к этой технологии. Он продемонстрировал миру потенциал и преимущества блокчейна. Впоследствии, на основе блокчейна и его усовершенствований, возникли альтернативные криптовалюты, а также новые направления использования этой технологии, не ограничивающиеся сферой цифровых валют [3].

Цифровая валюта – это любое средство платежа, представленное исключительно в виде цифровых данных. Эти деньги не имеют физической формы, а запись и перемещение средств происходит через интернет-платформы [4]. В ряде ситуаций их возможно конвертировать в традиционные денежные средства через банковские учреждения или терминалы самообслуживания.

Криптовалюта как правило – это цифровые валюты, функционирующие без единого регулирующего органа и предназначенные для применения в сети интернет. Криптовалюта предоставляет возможность проводить транзакции напрямую между пользователями, исключая необходимость в банках или платежных сервисах.

Технология блокчейн базируется на принципе распределенной базы данных, где регистрируются все транзакции. Эти данные структурированы в виде таблиц и верифицируются участниками сети в глобальном масштабе.

Данные в блокчейне обладают защитой от модификации и удаления, что придает технологии особую ценность. В связи с этим многие полагают, что блокчейн

способен устранить необходимость в посредниках и трансформировать существующие способы осуществления транзакций.

Эксперты анализируют вероятность упразднения должности нотариуса или существенные угрозы, которые технология блокчейн представляет для банковского сектора и пр. Большинство из них сходятся во мнении, что не следует спешить с окончательными заключениями. Нотариусы, вероятно, получат в распоряжение новый рабочий инструмент.

Блокчейн можно интерпретировать как обширную бухгалтерскую книгу. В настоящее время нотариусы являются держателями этих эксклюзивных книг, но в перспективе эти книги станут общедоступными в любой момент времени. Станет несложно удостовериться, существует ли идентичная запись у кого-либо еще и отсутствует ли в ней несоответствие.

В современном обществе входит в силу новая концепция: «Мир без посредников». Тем не менее можно с уверенностью утверждать, что число посредников и их воздействие на экономику будет сокращаться.

Хотя блокчейн вряд ли полностью вытеснит банки, нотариусов и другие аналогичные учреждения, его влияние на их функционирование несомненно.

В частности, банки, скорее всего, начнут фиксировать свои транзакции непосредственно в блокчейне. Это позволит клиентам продолжать пользоваться банковскими услугами, а сами кредитные организации смогут вносить данные в защищенный от изменений реестр.

Блокчейн открывает двери к разнообразным государственным сервисам, и опыт лидеров в этой сфере, таких как Эстония и отдельные эмираты ОАЭ, служит тому подтверждением.

Вполне вероятно, что уже при жизни нынешнего поколения активные граждане привыкнут к использованию блокчейна и основанных на нем идентификаторов.

Как в России, так и за рубежом правительства активно ищут пути для повышения эффективности своей работы. Перевод стандартных и устаревших процедур на блокчейн может стать перспективным решением. В то же время, вопросы конфиденциальности и защиты данных приобретают особую значимость в эпоху блокчейна.

Обеспечение защищенности информации – один из главных стимулов, подталкивающих медицинские учреждения к применению блокчейн-технологий. В условиях активной цифровизации здравоохранения организации все чаще внедряют инновационные решения для работы с медицинскими данными, преследуя цели повышения эффективности, качества обслуживания и прозрачности всей системы.

Блокчейн-решения в здравоохранении обладают гибкостью и могут быть настроены для решения широкого спектра задач [5]:

- управление информацией о пациентах – гарантирует полный контроль пациентов над их личными медицинскими записями;
- проведение клинических испытаний – обеспечивает проверку, координацию и строгое соблюдение утвержденных протоколов исследований;

- обработка претензий по оплате – создает понятную и прозрачную систему выставления счетов пациентам, используя смарт-контракты;

- отслеживание поставок лекарственных препаратов – позволяет установить подлинность лекарств и проследить всю историю их производства, помогая выявлять подделки.

Заметно, что блокчейн-технологии находят все большее применение в самых разных областях, что обусловлено их многочисленными преимуществами [6].

Одним из наиболее значимых плюсов блокчейна является его *децентрализованная структура*. Функционирование системы основано на распределенной сети, где отсутствует центральный орган управления. Это гарантирует повышенную безопасность и сопротивляемость кибератакам.

Другим существенным преимуществом блокчейна является *надежная защита информации*. В технологии используются криптографические методы для кодирования данных. Любая операция или запись в блокчейне фиксируется в виде уникального идентификатора – хеша. Это делает систему безопасной и предотвращает несанкционированные изменения или взлом.

Прозрачность также является важной характеристикой блокчейна. Это качество особенно ценно в тех сферах, где важны контроль и подтверждение истории операций. К примеру, в сфере поставок и логистики блокчейн позволяет проследить перемещение продукта от производителя до конечного потребителя.

Ни одна сеть не застрахована от атак, и блокчейн не является исключением. Однако, в отличие от традиционных сетей, распределенные реестры подвергаются специфическим угрозам. Злоумышленники стремятся повлиять на процесс достижения согласия, чтобы исказить данные, вносимые в реестр.

Несмотря на большое число участников блокчейна (например, около 11 тыс. узлов в сети Биткойн), блоки транзакций добавляются последовательно. Чтобы зафиксировать блок в цепочке, майнеры решают сложную вычислительную задачу. Тот, кто первым находит решение, получает право включить информацию о транзакциях в блокчейн. Майнеры мотивированы личной выгодой, так как за каждый найденный блок они получают вознаграждение (в настоящее время 12,5 монет в Биткойне).

Вычислительная задача не только сложна, но и ее результат должен соответствовать определенным критериям, например, формируемый хеш должен быть меньше целевого значения. Из-за этого крайне маловероятно, что два майнера одновременно найдут решение блока. Но такая ситуация все же может произойти. В этом случае оба участника сети отправляют свои блоки, и цепочка разделяется, образуя форк.

Сообщество продолжает майнить и добавлять новые данные в блокчейн. Каждый майнер связывает блок с той цепочкой, которую считает основной. Со временем становится ясно, какую цепочку сообщество признает действительной – она выбирается в качестве консенсуса.

Впоследствии небольшие форки забываются и игнорируются, а любая информация, добавленная в них, перерабатывается. Майнер, добавляющий блок к неактивной цепочке, не получает вознаграждения. Поэтому большинство майнеров игнорируют форки и поддерживают самую длинную цепочку.

Это подводит к понятию «атаки 51 %». Когда один участник (или группа) сосредотачивает в своих руках основную часть «голосов», он обретает возможность управлять консенсусом и вносить в блокчейн только выгодные ему данные.

Впрочем, даже незначительное превосходство над остальным сообществом не гарантирует успешное изменение уже зафиксированной информации. Злоумышленник может лишь добавлять блоки к желаемым ответвлениям. Следует понимать, что атака может быть осуществлена и с меньшими мощностями (менее 50 %), хотя шансы на успех существенно падают. В таких условиях злоумышленник может предпринять еще одну атаку, называемую «Double-spending»: потратить больше средств, чем реально имеется. Он создает несколько транзакций, используя одни и те же монеты. Теоретически сеть должна признать лишние транзакции недействительными и отклонить их, не включая в блок.

Однако, получив возможность размещать блок, злоумышленник может самостоятельно включить в него информацию с double-spending. Тогда честные майнеры создадут параллельную, валидную ветвь блокчейна, игнорируя блок атакующего. Но если злоумышленник контролирует 51 % вычислительных мощностей, он способен повлиять на консенсус и построить собственную цепь с «неверными» транзакциями, которая будет считаться «подлинной».

В истории известны примеры подобных атак. Так, блокчейны Ethereum Krypton и Shift подверглись атакам 51 % в августе 2016 г. Злоумышленники похитили монеты через double-spending. Впоследствии разработчики внедрили дополнительные механизмы защиты, например, в Krypton увеличили число подтверждений, необходимых для одобрения транзакции, до тысячи.

Атака Сивиллы, термин, заимствованный из медицинского описания пациентки с расстройством множественной личности, обозначает специфическую угрозу безопасности в сетевых системах. Суть атаки Сивиллы заключается в том, что один участник сети создает и использует множество поддельных идентификационных данных. Впервые это явление было подробно изучено и описано Джоном Дозье, исследователем из Microsoft.

Основной причиной уязвимости к атаке Сивиллы является сложность надежной идентификации физических устройств в сети. Различные методы, такие как отслеживание IP-адресов, использование уникального программного обеспечения или привязка к логинам и паролям, оказались неэффективными в предотвращении этой атаки.

Последствия атаки Сивиллы могут быть весьма серьезными. Она может использоваться для манипулирования результатами онлайн-голосований или для искусственного увеличения рейтинга веб-страниц в поисковых системах, например, в Google PageRank. В контексте блокчейн-технологий злоумышленник, проводящий атаку Сивиллы, стремится наводнить сеть множеством контролируемых им узлов. Это дает ему возможность блокировать транзакции, отключая пользователей от сети, а также повышает риск атаки 51 % и двойной траты средств. Кроме того, злоумышленник может получить возможность отслеживать все транзакции, используя специализированное программное обеспечение.

В централизованных системах защита от атак Сивиллы часто реализуется с помощью набора правил и ограничений. Например, система может ограничивать

количество аккаунтов, которые могут быть созданы с одного IP-адреса за определенный период времени.

DDoS-атака представляет собой разновидность кибернападения, при котором злоумышленники направляют огромный поток однотипных запросов на целевую систему. В архитектуре Биткойна предусмотрены механизмы для противодействия DDoS-атакам. Например, ограничение размера блока в 1 МБ служит для предотвращения перегрузки оперативной памяти полных нод. Также установлены лимиты на размер скриптов (до 10 000 байт), количество проверок подписей на блок (до 20 000) и число мультиподписей (до 20 ключей) [6].

Вдобавок, биткойн-клиенты автоматически блокируют любые узлы и транзакции, вызывающие подозрения. В последней версии клиента Bitcoin Core (ранее Bitcoin Satoshi) реализована функция логирования нестандартных транзакций, превышающих 100 килобайт. При обработке транзакций клиентская программа удостоверяется, что ни один из выходов не был использован ранее.

Блокчейн, нередко именуемый «двигателем истины», способствует устранению ряда сложностей, включая мошенничество и обман, однако не способен гарантировать абсолютную защиту в цифровом пространстве. В конечном счете эффективность блокчейна определяется участниками, применяющими его, и достоверностью информации, которую они в него загружают [7].

Список литературы

1. Арефьева А. С., Гогохия Г. Г. Перспективы внедрения технологии блокчейн // Молодой ученый. – 2017. – №. 15. – С. 326–330.
2. Белых В. С., Егорова М. А., Решетникова С. Б. Биткойн: понятие и тенденции правового регулирования // Юрист. – 2019. – №. 3. – С. 4–11.
3. Воронцова Е. А., Мелешенко Е. Г. Блокчейн: панацея или угроза для хранения и передачи информации // Синергия наук. – 2016. – №. 5. – С. 93–101.
4. Мащенко П. Л., Пилипенко М. О. Технология Блокчейн и ее практическое применение // Наука, техника и образование. – 2017. – №. 2 (32). – С. 61–64.
5. Пряников М. М., Чугунов А. В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International journal of open information technologies. – 2017. – Т. 5. – №. 6. – С. 49–55.
6. Ситник А. А. Цифровые валюты: проблемы правового регулирования // Актуальные проблемы российского права. – 2020. – №. 11 (120). – С. 103–113.
7. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.
8. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Фомичев С. А.¹,

*курсант факультета подготовки сотрудников
оперативных подразделений полиции Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Войде Е. Г.,

*старший преподаватель кафедры криминологии
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

КИБЕРПРЕСТУПНОСТЬ КАК НОВЫЙ ВЫЗОВ В КРИМИНАЛОГИИ

Киберпреступность представляет собой одну из наиболее острых и актуальных проблем современного общества, обусловленную стремительным развитием информационных технологий и увеличением зависимости от сети Интернет. С быстрым развитием информационных технологий мы вступили в новую эру преступлений, связанных с использованием компьютерных сетей. В этом контексте компьютеры и компьютерные сети становятся целью для злоумышленников, что подчеркивает важность понимания природы киберугроз. В эпоху цифровизации общества виртуальные угрозы стали неотъемлемой частью повседневной реальности, превратившись в серьезную проблему, которая затрагивает каждого пользователя сети. Растущая технологическая зависимость населения создает благодатную почву для деятельности киберпреступников, использующих современные IT-инструменты как оружие против финансовой и информационной безопасности граждан. С каждым днем цифровые злодеяния становятся все более изощренными: от банального фишинга до сложных схем социальной инженерии и DDoS-атак. Киберпространство превратилось в арену постоянной борьбы между хакерами и системами защиты, где каждая победа злоумышленников может обернуться серьезными последствиями для миллионов пользователей. Особую тревогу вызывает тот факт, что киберпреступность не знает границ и способна нанести удар по любой организации или частному лицу, независимо от их географического положения. При этом традиционные методы борьбы с преступностью часто оказываются бессильными перед лицом виртуальных угроз, что требует разработки новых подходов к обеспечению цифровой безопасности. Информационное общество, в котором мы живем, характеризуется активным взаимодействием его членов с информацией, включая ее переработку, хранение и распространение [3]. Это взаимодействие происходит в основном через интернет – сложную глобальную сеть, обеспечивающую обмен данными между пользователями по всему миру [4]. В условиях, когда Интернет пронизывает все сферы деятельности, киберпреступность представляет серьезную угрозу не только для отдельных граждан, но и для государств в целом.

¹ © Фомичев С. А., 2025.

Следует отметить, что преступления в сфере информационных технологий затрагивают не только личные, но и национальные интересы, что делает проблему кибербезопасности особенно важной для обеспечения стабильности и безопасности общества.

Ярким примером, иллюстрирующим опасность на государственном уровне, рассматриваемых преступлений, является, к примеру преступление, произошедшее в Чили. Там хакеры от имени Исламского государства взломали сайт министерства обороны страны. Взлом таких сайтов приводит к утечке данных, что влечет за собой катастрофические последствия. На территории нашей страны примеров киберпреступлений в последнее время является инцидент, связанный с Ларисой Долиной, когда по средствам связи мошенники представились представителями правоохранительных органов и путем обмана предложили ей перевести все денежные средства на безопасный счет, а также продать ее квартиру. Преступление носило длящийся характер, происходило на протяжении нескольких месяцев. Эти примеры показывают, что киберпреступления затрагивают как интересы государства, так и любого гражданина, и свидетельствуют о недостаточном уровне защиты от таких угроз.

Следующей острой проблемой является распространение порнографических материалов в сети интернет. Злоумышленники, используя мессенджеры (например, телеграмм каналы) или другие социальные сети распространяют материалы в закрытых каналах. На сегодняшний день, согласно статистическим данным МВД России, сохраняется тенденция к увеличению количества – на 28,7 % – противоправных деяний с использованием информационно-телекоммуникационных технологий. Их удельный вес в числе всех преступных посягательств возрос до 32,9 %, а по тяжким и особо тяжким – до 56,4 %. Лидируют преступления, которые совершаются дистанционно мошенниками. Раскрываемость киберпреступлений составила 29,9 %, в том числе совершенных с использованием сети Интернет – 28,8 %, расчетных (пластиковых) карт – 35,7 %. [7]. Данные цифры, несомненно, указывают на то, что разного рода киберпреступления стали одними из самых частых совершаемых противоправных деяний на территории Российской Федерации.

Таким образом, киберпреступления представляют собой преступления, совершаемые с использованием всемирной сети интернет и информационных телекоммуникационных технологий. Приведенные примеры также подтверждают, что как преступления, так и технологии постоянно развиваются и эволюционируют. Динамичное развитие технологий создает новые векторы для криминальной активности, при этом сами противоправные действия становятся все более сложными и изощренными, требуя от правоохранительных органов и специалистов по информационной безопасности соответствующего уровня подготовки и инструментария для эффективного противодействия.

Для преодоления комплекса проблем в данной сфере, на наш взгляд следует начать с законодательного закрепления понятия киберпреступности. Это связано с отсутствием в уголовном кодексе нормативно правового закрепления данного определения. Обращаясь к Уголовному кодексу РФ видим только перечень пре-

ступлений, относящихся к деяниям, совершенным с использованием информационно телекоммуникационными технологиями. Так, в уголовном кодексе есть глава 28 «Преступления в сфере компьютерной информации» [2]. Рассматривая ее, возникает вопрос: можно ли отнести перечисленные здесь преступления, а также приведенные ранее примеры, к категории киберпреступлений?

Чтобы ответить на этот вопрос, рассмотрим распространение порнографических материалов через интернет – ст. 272 УК РФ «Неправомерный доступ к информации» и ст. 242 УК РФ п. «б» ч. 3 этой статьи «Незаконные изготовление и оборот порнографических материалов или предметов с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети Интернет. Статья 272 УК РФ «неправомерный доступ к информации» посягает на общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями [6]. Как видно из данного объекта преступления в данном случае объектом посягательства является непосредственно отношения, обеспечивающие сохранность компьютерной информация. В статье 242 УК РФ непосредственным объектом преступления является нравственное здоровье населения, но при этом данное преступления совершается с помощью сети Интернет. Исходя из этого, мы видим, эти два преступления имеют разные объекты посягательства, но совершаются с использованием информационно телекоммуникационных технологий и сети Интернет.

В связи с этим можно утверждать, что к категории киберпреступлений относятся как правонарушения, регламентированные в главе 28 Уголовного кодекса Российской Федерации, так и противоправные деяния, осуществляемые с применением цифровых технологий, включая интернет-ресурсы, компьютерную технику и различные средства информационно-телекоммуникационного взаимодействия.

Таким образом, киберпреступления – это все преступные деяния, которые совершаются с использованием компьютера или информационно телекоммуникационных технологий. При этом важно отметить, что объект преступления в данном случае может быть разным. Например, как общественные отношения, обеспечивающие безопасность компьютерной информации (статья 272 УК РФ) или общественные отношения, затрагивающиеся при совершении такого преступления как «кардинг». Кардинг – это преступная деятельность, представляющая собой такой вид мошенничества, в котором происходят различные операции с банковскими картами с целью изобличения прибыли. Данное деяние наказывается по ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа». В ст. 159.3 УК РФ объектом преступления будут выступать общественные отношения, охраняющие право собственности. Из этого видно, что при совершении указанных деяний затрагиваются совершенно разные общественные отношения, однако оба они относятся к киберпреступлениям, поскольку осуществляются с использованием компьютеров и информационно телекоммуникационных технологий.

С учетом сложившейся политической обстановки нельзя обойти еще одну актуальную проблему, связанную с киберпреступлениями на данный момент. В настоящее время на территории Украины идет специально военная операция, это стало причиной увеличения мошеннических действий со стороны граждан Украины в отношении граждан Российской Федерации. Украинские мошенники, используя различные предлоги, склоняют россиян переводить им денежные средства. Однако на этом их преступная деятельность не заканчивается. С помощью шантажа они предлагают гражданам нашего государства совершать террористические акты, обещая вернуть деньги за эти действия. В результате за последнее время наблюдается рост поджогов военкоматов в России.

Таким образом, киберпреступность – это сложная и многогранная проблема, требующая внимания как со стороны государства, так и со стороны общества. Особую озабоченность вызывает тот факт, что киберпреступность затрагивает все сферы общественной жизни: от финансовых махинаций (как в случае с делом Ларисы Долиной) до государственной безопасности (взлом сайта министерства обороны Чили). Кроме того, наблюдается активное использование современных мессенджеров и социальных сетей для осуществления противоправной деятельности, что требует особого внимания со стороны правоохранительных органов. При этом необходимо отметить рост случаев киберпреступлений, исходящих с территории Украины и направленных против граждан Российской Федерации. Наблюдается существенное увеличение таких инцидентов с момента начала специальной военной операции. Государство должно вводить более эффективные меры по противодействию этим преступным деяниям.

В качестве первоочередного шага по противодействию киберпреступности представляется целесообразным законодательно закрепить само понятие киберпреступности в уголовном кодексе. Это позволит создать правовую основу для более эффективной борьбы с данным видом преступлений и адаптации законодательства к постоянно эволюционирующим технологиям и методам совершения противоправных действий в цифровом пространстве.

Таким образом, решение проблемы киберпреступности требует комплексного подхода, включающего совершенствование законодательной базы, усиление технической защиты и повышение осведомленности пользователей о потенциальных угрозах в цифровом пространстве.

Список литературы

1. Конституция Российской Федерации [Электронный ресурс] // URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 15.02.2025).
2. Уголовный кодекс Российской Федерации [Электронный ресурс] // URL: https://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/ (дата обращения: 16.02.2025).
3. Шестакова Е. Ф.Абрамова А. С. Эпоха интернет // ИТ портал. 2015. С. 2–4.

4. Павловец В. И. России нужны не биороботы, а креативный средний класс: о направлениях эффективного реформирования экономики и образования / В. И. Павловец // Альманах современной науки и образования. 2013 г. № 1 (68). С.103.

5. Информационный сайт РИА НОВОСТИ [Электронный ресурс] // URL: <https://ria.ru/amp/20241010/prestuplenie-1977435112.html> (дата обращения: 16.02.2025).

6. Официальный сайт генпрокуратуры [Электронный ресурс] // URL: <https://ria.ru/amp/20241010/prestuplenie-1977435112.html> (дата обращения: 17.02.2025).

7. Официальный сайт Министерства Внутренних Дел [Электронный ресурс] // URL: <https://мвд.рф/reports/item/41741442/> (дата обращения: 17.02.2025).

Хватова Я. Д.¹,

*курсант института подготовки сотрудников
для органов предварительного
расследования Московского университета
МВД России имени В.Я Кикотя*

Научный руководитель:

Михайленко Н. В.,

*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

СПОСОБЫ САМОЗАЩИТЫ ГРАЖДАН ОТ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Социальная инженерия, как метод манипуляции людьми с целью получения конфиденциальной информации, является одной из самых опасных угроз в современном мире. В отличие от традиционных методов преступности, преступления, связанные с социальной инженерией, зачастую не оставляют явных следов и могут быть совершены дистанционно. Применение таких методов становится все более распространенным в условиях цифровизации общества, когда большинство операций и коммуникаций происходят через электронные или информационно-телекоммуникационные сети, включая сеть Интернет. Проблема защиты граждан от преступлений, использующих методы социальной инженерии, приобретает все большую актуальность [1].

Целью данной статьи является анализ методов социальной инженерии, а также рассмотрение основных способов самозащиты граждан от преступлений, совершаемых с их использованием. Социальная инженерия – введение в заблуждение путем обмана или злоупотребления доверием для получения несанкционированного доступа к информации, электронным средствам платежа или побуждения владельцев самостоятельно совершить перевод денежных средств с целью их хищения [2]. Основными методами социальной инженерии являются фишинг, вишинг, смишинг, подмена личности.

Фишинг (phishing) – данный метод заключается в создании фальшивых сайтов, имитирующих официальные страницы банков, электронных магазинов,отовых операторов или государственных органов. Преступники отправляют фальшивые письма с просьбой перейти по ссылке и ввести личные данные.

Главной целью злоумышленников при использовании фишинга является получение конфиденциальных данных пользователей, в частности – логинов и паролей.

¹ © Хватова Я. Д., 2025.

Вишинг (vishing) – злоумышленники используют телефонные звонки, чтобы обманным путем получить конфиденциальную информацию. Обычно они представляются сотрудниками банка, правоохранительных органов или государственных учреждений и просят предоставить пароли, номера карт, коды или другую информацию.

Смишинг (smishing) – подобен фишингу, но использует SMS-сообщения для того, чтобы заставить жертву перейти по вредоносной ссылке или предоставить данные через текстовые сообщения. Подмена личности – преступники используют информацию о реальных людях (например, через социальные сети), чтобы представиться кем-то другим, например, знакомым, другом или родственником, попавшим в тяжелые жизненные обстоятельства, и убедить жертву раскрыть личные данные. Эти методы могут применяться как в одиночку, так и в комплексе, что увеличивает шансы злоумышленников на успех. Они давят на потерпевшего не только своей грамотностью и показным профессионализмом в той или иной области, но и оказывают психологическое и эмоциональное давление, а также часто манипулируют отсутствием времени, что воздействует на человека еще сильнее, толкая к более быстрому и поспешному принятию решения [3].

Именно поэтому самозащита от преступлений, совершенных с использованием методов социальной инженерии, требует комплексного подхода и формирования в сознании граждан понимания, что предотвращение преступлений зависит от их действий, произведенных до и во время контакта со злоумышленником.

Одним из наиболее эффективных методов защиты от социальных инженеров является повышение осведомленности граждан. Преступники, использующие методы социальной инженерии, часто рассчитывают на недостаток знаний жертв о возможных угрозах. Информационные кампании, обучение граждан безопасности в интернете и повышение их цифровой грамотности могут значительно снизить риски. Регулярные тренинги и семинары по вопросам безопасности в интернете, проводимые в школах, на рабочих местах и в общественных местах, могут помочь людям распознавать признаки фишинга, вишинга и других типов мошенничества. Проведение информационных кампаний, направленных на предупреждение о новых формах мошенничества, также помогает гражданам быть более настороженными.

Одним из самых эффективных способов защиты от преступлений, связанных с социальной инженерией, является использование двухфакторной аутентификации (2FA). Этот метод предполагает, что для входа в аккаунт пользователю нужно пройти два этапа аутентификации: сначала ввести пароль, а затем подтвердить свою личность с помощью второго фактора, например, через одноразовый код, отправленный на мобильный телефон.

Двухфакторная аутентификация значительно усложняет задачу преступников, так как даже если они получают доступ к паролю пользователя, без второго фактора (например, доступа к телефону) они не смогут воспользоваться данными [4].

Для защиты от фишинга и других видов социальной инженерии можно использовать антивирусное и антифишинговое программное обеспечение. Сове-

менные антивирусные программы и браузеры обладают функциями, которые автоматически блокируют фальшивые сайты, предупреждают о возможных угрозах и помогают избежать ошибок при вводе личных данных. Существуют также специальные плагины для браузеров, которые помогают распознавать фальшивые веб-сайты и предупреждают пользователей о возможных угрозах. Использование таких инструментов в значительной степени повышает безопасность онлайн-активности. Особое внимание следует уделить проверке информации, которая поступает от неизвестных источников. Преступники часто используют подмену личности, чтобы заставить жертву раскрыть личные данные. Прежде чем предоставить какую-либо информацию, важно удостовериться в том, что источник действительно является тем, кем он себя представляет. В случае с банковскими операциями, никогда не следует отвечать на телефонные звонки или письма, содержащие запросы на предоставление личных данных. Банки никогда не просят клиентов сообщать пароли или номера карт по телефону.

При получении сообщений с подозрительными ссылками следует всегда проверять их подлинность, обращая внимание на URL-адрес и характер письма.

Стать жертвой кибермошенников может любой человек. Тем не менее наибольший интерес для них представляют граждане, которые проявляют высокую экономическую активность и часто пользуются банковскими сервисами – люди в возрасте от 25 до 64 лет. Среди пострадавших наблюдается рост числа граждан старше 65 лет [5]. Старшему поколению и подросткам тяжело разбираться в программном обеспечении и следить за тенденциями развития различных видов мошенничества, поэтому данным категориям граждан необходимо придерживаться несколько другим способам самозащиты от преступлений, совершаемых с использованием методов социальной инженерии.

А именно: 1) как можно меньше публиковать личную информацию о себе в социальных сетях (в том числе паспортные данные, номер телефона, адрес); 2) не ставить одинаковые и простые пароли на учетные записи и аккаунты в социальных сетях и других сервисах; 3) записать все необходимые номера друзей, родственников и знакомых в телефонную книгу и не отвечать на незнакомые номера; 4) установить на телефон приложение, определяющее незнакомый номер (обычно такое приложение пишет «Спам/мошенники» на неблагонадежных номерах и разграничивает их от звонков сотовых операторов и интернет-провайдеров); 5) если с аккаунта друга просят срочно перевести деньги, то необходимо позвонить этому другу и проверить достоверность информации; 6) не сообщать никому коды, приходящие на телефон, а в случае прихода кода без запроса, обращаться в официальную поддержку банка или других организаций.

Преступники, использующие методы социальной инженерии, могут также использовать уязвимости в программном обеспечении для реализации своих планов. Для минимизации таких рисков важно регулярно обновлять операционные системы, программы и приложения. Современные версии программного обеспечения часто содержат патчи и исправления для устранения уязвимостей, которые могут быть использованы злоумышленниками.

Преступления, совершенные с использованием методов социальной инженерии, представляют собой одну из самых серьезных угроз для граждан в современном цифровом обществе. Понимание этих угроз и принятие эффективных мер защиты может значительно снизить риск стать жертвой мошенников. Повышение осведомленности, использование двухфакторной аутентификации, антифишингового программного обеспечения, тщательная проверка источников информации и регулярное обновление программного обеспечения – все эти меры в комплексе могут обеспечить надежную защиту от преступлений, совершаемых с использованием социальной инженерии. Тем не менее несмотря на существующие методы защиты, важно помнить, что преступники постоянно совершенствуют свои техники. Поэтому важно продолжать обучение и обновление знаний в области цифровой безопасности, чтобы эффективно противостоять новым угрозам.

Список литературы

1. Основные направления развития финансового рынка Российской Федерации на 2023 год и период 2024 и 2025 годов (разработаны Банком России). URL: https://www.consultant.ru/document/cons_doc_LAW_435343/.
2. Барабанов П. А. Информационная безопасность личности: проблемы и пути их решения // Информационное право. – 2022. – № 2. – С. 12–17.
3. Гребенюк О. С. Современные угрозы цифровой безопасности и методы противодействия социальной инженерии // Вестник Томского государственного университета. – 2021. – № 465. – С. 95–102.
4. Дмитриева И. А. Преступления в сфере высоких технологий: криминологические и правовые аспекты. – М.: ЮНИТИ-ДАНА, 2020. – 248 с.
5. Зверев Д. Ю. Защита от фишинга и социальной инженерии в корпоративной среде // Информационные технологии и безопасность. – 2023. – № 1 (55). – С. 37–42.
6. Литвинова Е. Г. Фишинг как способ социальной инженерии: правовая оценка и меры противодействия // Правовая инициатива. – 2022. – № 3(73). – С. 61–66.
7. Мартынов А. А. Социальная инженерия: психология манипуляции и методы защиты. – СПб.: Питер, 2021.
8. Носкова И. В. Психологические механизмы социальной инженерии и возможности их нейтрализации // Вопросы психологии. – 2020. – № 6. – С. 103–110.
9. Паньшин В. Н. Комплексный подход к защите от социальной инженерии в информационной безопасности // Современное право. – 2023. – № 4. – С. 77–82.
10. Федотов К. Н. Противодействие кибермошенничеству: правовые и организационные меры. – М.: Проспект, 2021. – 224 с. Шилова И. А. Цифровая грамотность как фактор снижения киберпреступности // Информационное общество. – 2023. – № 2. – С. 45–50.

11. Кибермошенничество: портрет пострадавшего Центральный Банк России
URL: https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/.
12. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.
13. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Черникова М. В.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Михайленко Н. В.,

*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ МАССИВАМИ ДАННЫХ BIG DATA

Искусственный интеллект (ИИ) и Big Data (большие данные) – концепции, укоренившиеся в технологической повестке десятилетия назад. Однако их комплексность продолжает оставаться вызовом для бизнеса: как показывают исследования, многие организации осознают отставание в реализации этих технологий и связанные с этим риски для долгосрочной конкурентоспособности [1].

Применение ИИ в управлении Big Data подразумевает использование алгоритмов машинного обучения, позволяющих извлекать скрытые закономерности из массивов информации. Эти взаимодополняющие технологии формируют основу «когнитивной революции» в бизнес-аналитике. Если Big Data обеспечивают сырьевую базу – гигантские объемы структурированных и неструктурированных данных, – то ИИ выступает инструментом их трансформации в стратегически значимые инсайты. Согласно опросу 2023 г., 76,5 % экспертов подтверждают синергию технологий: ИИ требует данных для обучения, а Big Data – интеллектуальных систем для интерпретации [1].

Симбиоз технологий в бизнес-процессах Интеграция ИИ и Big Data кардинально меняет подходы к управлению. Например, в розничной торговле традиционное прогнозирование спроса, основанное на исторических данных, уступает место предиктивным моделям. Анализ поведения клиентов в реальном времени, данных с кассовых терминалов и соцсетей позволяет повысить точность прогнозов на 50 %. Это достигается за счет:

1. Глубинного обучения (нейросети выявляют неочевидные корреляции).
2. Обработки потоковых данных (IoT-устройства, геолокация).
3. Автоматизации решений (динамическое ценообразование, управление запасами).

Таким образом, симбиоз ИИ и Big Data открывает путь к «умному» управлению, но требует системных инвестиций в технологии, кадры и нормативную

¹ © Черникова М. В., 2025.

базу. Ключевой тренд будущего – переход от анализа данных к их когнитивной интерпретации в режиме реального времени.

Внедрение технологий Big Data позволяет компаниям прогнозировать угрозы на ранних этапах, оценивать масштабы потенциального ущерба и оперативно адаптироваться к вызовам. Например, предиктивные модели на основе машинного обучения помогают не только минимизировать рыночные и потребительские риски, но и моделировать сценарии реагирования на форс-мажоры – от экономических кризисов до природных катастроф [1].

Анализ цифровых следов пользователей (истории покупок, поведение на сайте, геолокация) открывает возможности для гипертаргетированного маркетинга. Интеграция данных из CRM-систем, соцсетей и IoT-устройств в единое «озеро данных» позволяет: выявлять скрытые предпочтения аудитории, оптимизировать рекламные кампании в режиме реального времени, увеличить конверсию на 15–20 % за счет персонализированных предложений.

Современные аналитические платформы способны:

1. Фиксировать отклонения в работе IT-систем (несанкционированный доступ, DDoS-атаки).
2. Выявлять паттерны мошенничества (подозрительные транзакции, фишинг).
3. Прогнозировать угрозы с точностью до 92 % на основе исторических данных [1].

Как справедливо отмечают Е. В. Пастухов и Ю. С. Романов, интеграция ИИ и Big Data требует пересмотра бизнес-процессов [2]. Однако ключевая проблема, по мнению Д. В. Сикулера, – дефицит кадров: лишь 12 % компаний имеют штатных data scientists. Решением становятся SaaS-платформы с готовыми алгоритмами, которые: автоматизируют ETL-процессы (извлечение, преобразование, загрузка данных), упрощают анализ через drag-and-drop интерфейсы, снижают затраты в 3–5 раз по сравнению с разработкой собственных решений [3].

Большинство компаний, вовлеченных в цифровой маркетинг, уже сталкивались с алгоритмами машинного обучения (МО) при работе с Big Data. Как подчеркивают Дж. Уилсон и коллеги, технологические гиганты, такие как Google, стали пионерами в применении МО для гиперперсонализации рекламных кампаний, что напрямую влияет на их эффективность [4].

Преимущества интеграции ИИ и Big Data Зарубежные исследователи единодушны: симбиоз ИИ и больших данных создает стратегические преимущества. По словам К. Панетты, «интеллектуальная аналитика трансформирует принятие решений, повышая точность управленческих действий» [5]. Эти возможности масштабируются в зависимости от бизнес-задач:

Оптимизация операций (прогнозирование спроса, логистика);

1. Стратегическое планирование (определение приоритетов сбора данных).
2. Инновации (разработка продуктов на основе поведенческих инсайтов).

Современные организации осознают, что данные содержат ответы на ключевые вопросы конкурентоспособности. Управление без их анализа аналогично навигации в темноте: решения принимаются интуитивно, а не на основе фактов.

Как показывает практика, компании, внедрившие data-driven подход, демонстрируют на 30 % более высокую рентабельность [5].

Интеграция ИИ в аналитику перестает быть опцией – это необходимость. С развитием облачных платформ и low-code решений (например, Microsoft Azure ML) даже малые предприятия получают доступ к продвинутым алгоритмам. Эксперты прогнозируют, что к 2026 г. 85 % компаний будут использовать ИИ-аналитику как часть стандартных бизнес-процессов [4].

Риски отказа от внедрения ИИ и Big Data Компании, игнорирующие интеграцию интеллектуальной аналитики, неизбежно столкнутся с потерей конкурентных преимуществ. Как показывают исследования McKinsey, организации, использующие data-driven подход, демонстрируют на 23% более высокую операционную эффективность по сравнению с традиционными игроками [1]. Стратегические решения, основанные на предиктивной аналитике, позволяют:

1. Оптимизировать бюджетные расходы (снижение издержек на 15–30 %).
2. Минимизировать риски ошибочных инвестиций.
3. Формировать долгосрочные прогнозы с точностью до 85 % [2].

Эволюция аналитических инструментов свидетельствует: алгоритмы ИИ становятся обязательным элементом бизнес-архитектуры. К 2026 г., по данным Gartner, 90 % корпораций будут использовать ML-модели для обработки данных, а их отсутствие в стратегии станет фактором рыночной маргинализации [3].

Выводы и рекомендации:

1. Приоритизация технологий – интеграция ИИ и Big Data должна занимать топ-3 в списке стратегических целей компании.
2. Доступность решений – облачные платформы (Google AI Platform, Microsoft Azure ML) снижают порог входа: даже малые предприятия могут внедрять сложные алгоритмы без штатных data scientists.
3. Конкурентное выживание, как отмечает К. Панетта, «отказ от интеллектуальной аналитики к 2030 г. будет равносителен добровольному выходу из рынка» [4].

Список литературы

1. Яндекс: Искусственный интеллект для управления большими данными Big Data [Электронный ресурс]. – Режим доступа: <https://yandex.ru/vc.ru/u/1266146-404/550756> (дата обращения: 11.05.2025).
2. Пастухова Е. В. Искусственный интеллект: исследования в эпоху Big data / Е. В. Пастухова, Ю. С. Романова // Волновая электроника и инфокоммуникационные системы : Сборник статей XXV Международной научной конференции. В 3-х частях, Санкт-Петербург, 30 мая – 03 2022 года. Часть 3. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2022. – С. 81–85. – EDN MDRZCZ.
3. Сикулер Д. В. Ресурсы, предоставляющие данные для машинного обучения и проверки технологий искусственного интеллекта / Д. В. Сикулер //

Информационные и математические технологии в науке и управлении. – 2021. – № 2 (22). – С. 39–52. – DOI 10.38028/ESI.2021.22.2.004. – EDN RCBUHR. Уилсон Дж., Догерти П. Р. Люди и искусственный интеллект объединяют усилия // Harvard Business Review. 2018. № 96. С. 115–123.

4. Панетта К. Топ-10 стратегических технологических трендов на 2023 ГОД/ URL: <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technologytrends-for-2018> (дата обращения: 11.05.2025).

5. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

6. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Шапаев М. С.¹,

*слушатель института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Пушкарёв В. В.,

*начальник кафедры противодействия преступлениям
в сфере информационно-телекоммуникационной среде
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ, СКЛАДЫВАЮЩИЕСЯ НА ПЕРВОНАЧАЛЬНОМ И ПОСЛЕДУЮЩЕМ ЭТАПАХ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ ИНТЕРНЕТ

Приоритетным и актуальным направлением деятельности правоохранительных органов является организации противодействия преступлениям, совершаемых с использованием ИТС, включая сеть Интернет. Ежегодно на расширенных коллегиях МВД России поднимается вопрос о совершенствовании и оптимизации работы всех подразделений по этому направлению. Организация противодействия преступлениям заключается в повышении уровня защищенности личности, общества и государства в целом, а также в снижении показателей противоправного использования ИТС, цифровых технологий и ликвидации последствий кибератак на критическую информационную инфраструктуру, компьютерную информацию и кредитно-финансовую сферу.

Отсутствие унифицированных методик по расследованию преступлений, совершаемых с использованием ИТС, включая сеть Интернет затрудняет всестороннее расследования уголовных дел в виду многообразия и изменчивости следственных ситуаций. Ввиду этого органы предварительного следствия ставят перед собой цель по увеличению раскрываемости данной категории преступлений по средствам совершенствование организационных, тактических и методических основ.

Одним из способов достижения подобной цели является планомерное составление и отработка типичных следственных ситуаций. Под типичными следственными ситуациями понимается наиболее часто встречающиеся сочетание условий, создающих определенные, наиболее вероятные для данного вида преступлений обстоятельства, которые определяют применения отдельных положений методики расследования. Последовательность первоначальных следственных

¹ © Шапаев М. С., 2025.

действий предопределяется характером следственной ситуации на первоначальном этапе. Проанализировав вышеуказанное понятие, можно дифференцировать два аспекта, служащих для определения следственной ситуации. Во-первых, познавательный аспект, выступающий оценочной категорией для принятия процессуального решения, во-вторых, информационный, представляющий собой объем информации необходимый для дальнейшего расследования [1]. Содержание следственной ситуации формируется на основании совокупности компонентов. Психологические, то есть проявление участниками уголовного судопроизводства психологического противодействия или содействия следствию. Организационно-технические, наличие или отсутствие у следователей технических и организационных средств для оперативного реагирования, проведения следственных действий, а также для следственного маневрирования с помощью различных инстументариев, оптимизирующих их деятельность. Информационные – совокупность обнаруженных, изъятых и исследованных следов преступного посягательства, выступающих в качестве доказательств, а также иные информационные источники, полученные в ходе следственных действий или ответов на запросы. Процессуальные и тактические, представляющие собой возможность и целесообразность избрания конкретной меры пресечения, а также необходимость и фактическая возможность проведения оперативно-розыскных мероприятий или следственных действий).

Классификация следственных ситуаций по преступлениям с использованием ИТС, включая сеть Интернет разнообразна. Криминалист Н. И. Старостенко в своих трудах систематизировал следственные ситуации следующим образом [2].

По источнику информации о совершенном преступлении выстраивают следственные ситуации, когда преступление обнаружено владельцем или пользователем охраняемой компьютерной информации. Как правило, данный способ обнаружения присущ коммерческим и кредитно-банковским организациям, объектам критической информационной инфраструктуры (далее – КИИ), где противоправные воздействия на компьютерную информацию выявляют сотрудники службы безопасности, в ходе проверок либо по средствам систем программного обеспечения. Согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) предназначена решать задачи обеспечения безопасности КИИ России.

Преступные посягательства выявляются в процессе производства следственных действий, в ходе проведения оперативно-розыскных мероприятий и проверок со стороны органов прокуратуры. Так, например, в ходе мониторинга и блокировки незаконно размещенных объявлений в теневой сети Интернет, в октябре 2024 г. сотрудниками управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий (далее УБК) была пресечена деятельность по продажам доступов к неправомерному дистанционному банковскому обслуживанию (далее – ДБО). В ходе предварительного

следствия было установлено, что лицом, размещающим объявление в darknet являлся сотрудник службы безопасности коммерческого банка, который в соответствии со своим должностным регламентом имел доступ к СМС оповещению клиентов. Сотрудник осуществлял продажу базы данных с номерами телефонов. Лица, приобретавшие данные абонентские номера по средствам восстановления пароля через двухфакторную аутентификацию получали доступ к мобильному банковскому приложению [3].

В зависимости от объема информации, которая имеется в распоряжении правоохранительных органов. Во-первых, отсутствуют сведения, касающиеся способа, мотива, личности преступника, но при этом последствия преступного деяния известны. Во-вторых, органы предварительного расследования располагают информацией, связанной с мотивами, способами и личностью преступника, но при этом лицо не задержано, такие следственные ситуации носят характер очевидной направленности. В-третьих, распространенная сложившаяся следственная ситуация, когда имеются последствия противоправного деяния, известны мотивы, способы совершения преступления, но отсутствуют какая-либо характеристика о лице, совершившем преступление.

Проверка сообщения о преступлении по данной категории уголовных дел складывается из ряда процессуальных и оперативно-розыскных действий, как сбор информации о лице, чья компьютерная информация была уничтожена, заблокирована, копирована, модифицирована, определение характера и объема информации, на которую направлено преступное посягательство, путем опроса причастных лиц, осмотр места происшествия с последующим изъятием электронных носителей информации при необходимости или копирования их образов, истребование документов и предметов, подтверждающие право пользования, владения и распоряжения технических устройств или компьютерной информации, привлечение специалистов для более планомерного проведения отдельных следственных действий, а также с целью консультации, назначение различных видов судебно-компьютерных экспертиз и дача поручений органу дознания на установление лиц, совершивших преступления и их местонахождения. Для дальнейшего описания организационных, тактических и методических особенностей расследований преступлений с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» следует выбрать одну из самых распространенных следственных ситуаций, когда неизвестен субъект противоправных деяний, имеются обстоятельства совершения преступления, сведения о преступном посягательстве на компьютерную информацию, потерпевшем и последствиях в целом.

Не каждая следственная ситуация, складывающаяся на первоначальном этапе расследования, предполагает очевидность места совершения преступления [4]. В правоприменительной практике по уголовным делам с использованием ИТС, включая сеть Интернет часто признается местом совершения преступления отделение банка, где был открыт счет, либо откуда велся электронный учет электронных денежных средств без открытия счета. В зависимости от следственной ситуации, например, при совершении преступления, предусмотренного ст. 272 УК РФ место совершения преступления может определяться по средствам IP-

адреса, MAC-адреса или IMEI, но следует учитывать возможное использования преступниками зарубежных серверов VPN и проху. Таким образом, комплексное определение места совершения преступления, предусмотренного главой 28 УК РФ, требует тщательного анализа следственных ситуаций на первоначальном этапе расследования.

В криминалистической литературе по-разному оценивается значение первоначального этапа расследования. Ряд криминалистов акцентируют внимание на организационно-тактические и методические значения первоначального этапа и считают его приоритетным, недооценивая последующий. Вызвана данная тенденция тем, что в методических рекомендациях, учебных пособиях отражены не в полном объеме следственные ситуации, организация и проведение следственных действий на последующем этапе, либо ограничиваются незначительным количеством комментариев. По нашему мнению, описывая перечень и особенности тактики следственных действий, и их сочетание с оперативно-розыскными мероприятиями в учебной литературе должны уделять должное одинаковое внимание двум этапам расследования.

В следственных ситуациях, сложившихся на первоначальном этапе расследования, где известен объект преступного посягательства, последствия, но не установлен субъект, необходимо в соответствии со ст. 144 УПК РФ дать поручение сотрудникам оперативных подразделений на установление местонахождение лица, совершившего преступление. В частности, управлению по организации борьбы с противоправным использованием информационно-коммуникационных технологий, бюро специальных технических мероприятий, а также четвертому отделу уголовному розыска, который курирует специализированные отделы «Дистанционные хищения», следует учитывать достоверность и допустимость доказательств, путем изучения предоставляемого рапорта о проведении оперативно-розыскных мероприятий. Также первоначальный этап предполагает эффективное взаимодействие с работниками негосударственных и финансово-кредитными организациями. В подразделениях, осуществляющих предварительное следствие с октября 2023 г. установлена автоматизированная система ФинЦЕРТ Банка России, целью которой является мониторинг и отслеживания банковских операций без согласия клиента, обмен данными происходит с соблюдением норм банковской тайны. Сведения, которые ФинЦЕРТ получает от правоохранительных органов, впоследствии учитываются системами банков для предотвращения новых кибератак на кредитно-финансовую сферу.

В случаях, когда возникает необходимость своевременно установить лиц, осуществивших преступные посягательства на кредитно-финансовую сферу, сотрудники предварительного следствия пользуются разработкой по предоставлению государственных сведений, с помощью которой возможно в кратчайшие сроки отправить запрос на получение выписки о движении денежных средств по счету в банковские организации и постановление о возбуждении перед судом ходатайства на получение информации о соединениях между абонентами и (или) абонентскими устройствами в операторы сотовой связи, при-

крепляя данное постановление судебным решениям с целью получения расширенной детализации для дальнейшего проведения такого оперативно-розыскного мероприятия как снятие информации с технических каналов связи.

Оценив и описав значимость первоначального этапа расследования, планомерным образом следует перейти к изучению следственных ситуаций, сложившихся на последующем этапе расследования преступлений, совершаемых с ИТС, включая сеть Интернет. Следственные ситуации, описывающие характер отношений и складывающиеся на последующем этапе, могут быть конфликтными и бесконфликтными.

Конфликтные следственные ситуации характеризуют процесс расследования с точки зрения иных, частных обстоятельств, например, оказываемого противодействия подозреваемым или обвиняемым следователю и суду. Конкретная следственная ситуация отражает индивидуальность и своеобразие последующего этапа расследования. Например, лица, участвующие в досудебном производстве, отказываются от дачи показаний, меняют их или дают заведомо ложные, то есть в данной ситуации интересы и цели следователя с участником уголовного дела не совпадают. Следственные ситуации, с которыми сталкиваются правоохранительные органы на последующем этапе расследования преступлений с использованием ИТС, включая сеть Интернет, разнообразны в виду способов преступных деяний.

Примером следственной ситуации на последующем этапе расследования является случай, когда лицо, совершившее преступление установлено, ряд характеризующего материала на него собрано, известны способы совершения преступления, но его местонахождение по-прежнему неизвестно. Например, информация, полученная в ходе проверки сообщения о преступлении проанализирована и дает основания полагать, что группа, действовавшая по предварительного сговору, путем неправомерного доступа к компьютерной информации по средствам ее копирования получили доступ к аккаунту криптокошелька на криптобирже, вследствие чего похитили 2 единицы такой криптовалюты как Ethereum. На данном этапе расследования необходимо установить факт и способ «распыления», то есть перевод криптовалюты на кошельки предполагаемых дропов, как правило данная процедура совершается с помощью криптовалютных миксеров, представляющих собой сервисы по смешиванию криптовалюты разных владельцев, что затрудняет установить их источник происхождения. На сегодняшний день выделяют следующие криптомиксеры: децентрализованные, которые используют протоколы типа CoinJoin, основанные на скоординированных и одноранговых (P2P) подходах (Yomix.io, Unijoin) и централизованные кастодиальные (Coinomize). Одним из способов получения данной информации могут послужить инструменты коммерческой деятельности по мониторингу и отслеживанию транзакций криптовалют. Так, например, следователи в своей деятельности прибегают к эксплореру, созданный компанией АО «ШАРД» для онлайн-поиска, агрегирования и анализа общедоступных данных из различных блокчейнов и иных доступных источников информации. С его помощью представляется возможным анализировать все, что

построено на технологии публичного блокчейна: криптовалюты, смарт-контрактов, NFT-токенов и операций с ними. Результат поиска органам предварительного следствия представляются в графическом интерфейсе, и автоматически генерируемых онлайн-отчетах, что в совокупности позволяет определить количество и вид цифровых активов, даты и время осуществляемых транзакций, получателей и отправителей криптовалюты. После сбора и анализа, имеющихся сведений о лице, которому поступила криптовалюта, сотрудники правоохранительных органов направляют запрос в биржу, которой обслуживается проверенный адрес владельца кошелька. Как правило, представители бирж оказывают содействие при виде письма, отправленного с официального домена МВД России, а также факта возбужденного уголовного дела и беспрепятственно отправляют расширенный детализированный отчет в zip-файле, внутри которого содержится Excel-таблица с указанием получателей, дат и времени переводов и личных сведений владельца кошелька (паспортные данные).

Данная методика позволяет сотрудникам предварительного следствия в кратчайшие сроки определять местонахождения конвертируемых денежных средств и накладывать на них арест, для обеспечения гражданского иска потерпевших. При составлении запроса в биржу необходимо прописать информацию, интересующую следователя для всестороннего и полного исследования обстоятельств уголовного дела, а именно: завершённые сделки, расширенную выписку движения всех криптовалют, с указанием счетов (ник-неймов, криптокошельков, сведений о верификации и полные анкетные данные участников сделки), актуальный абонентский номер, актуальные дебетовые банковские карты, фотографии при наличии если аккаунт был верифицирован, историю с каких ip-адресов были осуществлены входы в систему, сведения о пополнении кошелька в офисе биржи, видеозапись (при наличии), сведения о доверенности выданной для пополнения и управления счетом, а также данные доверенных лиц.

После получения ответа, органам предварительного следствия в кратчайшие сроки требуется проанализировать финансовые операции лиц и построения финансовых связей между, интересующими следствие участниками и вынести постановление о возбуждении перед судом ходатайства о наложении ареста на имущество, в связи с тем, что промедление в производстве ареста на указанные денежные средства может повлечь их утрату и обеспечить продолжение незаконной деятельности неустановленного лица.

В этой связи возникает проблема, с которой сталкивается следователь, а именно отсутствие возможности использовать подобные инструменты при расследовании преступлений, так как имеющиеся специализированные компьютерные программы и оборудование не отвечают предъявляемым к ним требованиям как технико-криминалистическим средствам. По нашему мнению, путем преодоления сложившейся следственной ситуации является привлечение специалиста в соответствии со ст. 168 УПК РФ, ввиду наличия у него специальных знаний или путем получения подобного рода сведений через оперативных сотрудников по средствам, предоставленного ими рапорта.

Известно, что последующий этап расследования преступлений с использованием ИТС, включая сеть Интернет сопровождается регулярным продлением сроков предварительного следствия в соответствии со ст. 162 УПК РФ и постоянными жалобами со стороны потерпевших, связанных с возвращением их имущества. Следователям приходится докладывать о всей проделанной работе по средствам справок, в которых указываются следственные действия, проведенные на момент ее составления, поручения оперативным подразделениям, а также список планируемых мероприятий.

Л. Я. Драпкин, заложивший основы теории следственной ситуации, определяет ее как «мысленную динамическую модель, отражающую информационно-логическое, тактико-психологическое, тактико-управленческое и организационное состояние, сложившееся по уголовному делу. По нашему мнению, данную интерпретацию, применяемую к понятию следственной ситуации, возможно дополнить, используя ИТС, включая сеть Интернет, при совершении преступлений, как факультативный аспект состояния следственной ситуации, усложняющий процесс расследования как на первоначальном этапе расследования, так и на последующем.

Список литературы

1. Марьясис И. В. Криминалистические характеристики компьютерных преступлений // Инновационная наука. 2021. № 12-2. С. 18.
2. Харина Е. А. Типовые следственные ситуации первоначального этапа расследования мошенничества в сфере компьютерной информации // Закон и право. 2023. № 11. С. 273.
3. Никеров Д. М., Хохлова О. М. Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института МВД России. 2023. № 2 (89). С. 90.
4. Чекунова И. Г. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учебное пособие. М.: Проспект, 2023. С. 17.
5. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.
6. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Шибаров Н. А.¹,
*курсант института подготовки
сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Поликарпова Е. В.,
*старший преподаватель
кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя*

ТЕНЕВОЙ ИНТЕРНЕТ: ДАРКНЕТ МЕЖДУ УГРОЗОЙ И СВОБОДОЙ

Ежедневно миллиарды пользователей взаимодействуют с поверхностным слоем интернета, даже не подозревая о существовании скрытого цифрового мира – Даркнета. Этот сегмент, название которого отражает его суть («dark» – «темный», «net» – «сеть»), остается недоступным для обычных браузеров [1]. Для входа требуются специализированные инструменты: браузер TOR, сети I2P или VPN. Истоки Даркнета восходят к ARPANET, созданной для военных и научных целей, но современное название закрепилось в 2002 г. благодаря сотрудникам Microsoft.

Даркнет часто ассоциируется с незаконной деятельностью, но его сущность сложнее. Эксперты разделяют понятия DarkNet и DarkWeb: первый – это инфраструктура анонимных сетей, второй – ресурсы для нелегальных операций. В DarkNet можно найти независимые СМИ, форумы для диссидентов, приватные почтовые сервисы, тогда как DarkWeb – это черные рынки, где торгуют наркотиками, оружием, поддельными документами и украденными данными. Анонимность, главный козырь Даркнета, одновременно служит щитом для свободы слова и инструментом преступников, усложняя работу правоохранительных органов.

Ключ к анонимности – технологии вроде браузера TOR, который маскирует IP-адрес, направляя трафик через цепочку узлов. Его интерфейс напоминает Firefox, но домены здесь заканчиваются на «.onion», а функционал включает обход цензуры, защиту в публичных сетях Wi-Fi и доступ к скрытым сайтам. Однако анонимность не абсолютна: человеческие ошибки, уязвимости в ПО или слежка на стыке сетей могут раскрыть личность. Как отмечает эксперт Дмитрий Галов, «дистанционно отследить действия пользователя в Даркнете почти невозможно, но сам факт входа оставляет цифровые следы».

¹ © Шибаров Н. А., 2025.

Преступления в Даркнете поражают разнообразием. На первом месте – онлайн-маркетплейсы вроде закрытого магазина Mega, где под видом легальных товаров продают наркотики, оружие и данные жертв фишинга. Киберпреступления включают кражу личных данных, распространение вредоносного ПО и шантаж. Например, вирусы-шифровальщики, блокирующие доступ к файлам, часто разрабатываются и продаются в DarkWeb. Отдельная угроза – детская порнография, которую правоохранители пытаются искоренить через международное сотрудничество и мониторинг трафика.

Даркнет также стал ареной кибершпионажа и политических манипуляций. Утечки секретных документов, как расстрел журналистов в Ираке, вскрытые через DarkNet в 2003 году, демонстрируют его роль в разоблачении власти [2]. Однако террористические группы используют те же инструменты для координации атак, как во время «арабской весны», где анонимные каналы способствовали дестабилизации целых государств.

Попытки контроля над Даркнетом сталкиваются с дилеммой: как бороться с преступностью, не нарушая права на приватность [3]. Технологии деанонимизации, анализ паттернов трафика и внедрение «цифровых отпечатков» в криптовалютные транзакции уже помогли закрыть ряд рынков, например, Silk Road. Но радикальные меры, вроде полной блокировки TOR, рискованны – они лишат защиты диссидентов и журналистов в авторитарных режимах.

Высокий уровень анонимности и шифрования в DarkNet создает у злоумышленников ложное ощущение безопасности, что способствует широкому спектру противоправной деятельности. В этой скрытой сети функционируют маркетплейсы, аналогичные легальным платформам вроде Ozon или Wildberries, но специализирующиеся на незаконных товарах. Например, магазин Mega открыто торгует наркотиками, тогда как другие предлагают оружие, поддельные документы, данные украденных кредитных карт, запрещенные вещества, а также услуги киберпреступников – от взломов до кражи личных данных. Подобная активность не только нарушает закон, но и формирует угрозы для общества, провоцируя рост преступности и подрывая общую безопасность.

Киберпреступления в DarkNet включают кражу персональной информации через фишинговые схемы, после чего данные продаются заинтересованным лицам. Злоумышленники также приобретают вредоносные программы для атак на системы, а используя доступ к конфиденциальной информации, шантажируют жертв, требуя выкуп. Отдельную опасность представляет распространение порнографического контента, в том числе с участием несовершеннолетних, что не только незаконно, но и наносит моральный ущерб обществу. Анонимность DarkNet позволяет преступникам безнаказанно эксплуатировать такие материалы, создавая риски для детей и поощряя нарушения этических норм [4]. Эти факторы делают DarkNet площадкой для систематических нарушений, привлекающих внимание правоохранительных органов и требующих комплексных мер противодействия.

Таким образом, Даркнет остается двойственным феноменом. С одной стороны, это убежище для торговли смертью, эксплуатации детей и кибертерро-

ризма. С другой – инструмент борьбы за свободу информации и спасения жизней, как в случае с активистами, скрывающимися от преследований. Его будущее зависит от баланса между безопасностью и правами человека: ужесточение регулирования должно сопровождаться развитием технологий защиты анонимности для тех, кто в ней действительно нуждается. Как и Интернет в начале 90-х гг., Даркнет – это не добро и не зло, а зеркало, отражающее амбиции и страхи общества.

Теневой сегмент интернета является большой угрозой для национальной безопасности Российской Федерации. Это обусловлено тем, что данную сеть практически невозможно контролировать из-за ее высокого уровня защиты и шифрования. Спец службам разных стран крайне тяжело отслеживать и выявлять пользователей, связанных с незаконной деятельностью. Будь то продавцы или покупатели маркетплейсов, распространители снафф-видео и иного негативного контента. Отследить IP-адреса пользователей проблематично из-за очень большого количества переадресаций при подключении пользователя к серверам. Незаконная предпринимательская деятельность предоставляет угрозу для общества, поскольку распространение оружия, психотропных или наркотических веществ приводят к дестабилизации и росту преступности. Происходит рост убийств, случаев насилия, грабежей, разбойных нападений и многих других тяжких преступлений [5]. Это в свою очередь значительно усложняет работу правоохранительных органов и подрывает доверие со стороны населения.

Список литературы

1. Даркнет: что это, запрещено ли входить из России в 2025 году, что можно делать через браузер, как он выглядит – Hi-Tech Mail // URL: <https://hi-tech.mail.ru/news/50786-kak-popst-v-darknet/>.
2. История зарождения даркнета: от военных лабораторий до Tor Browser // URL: <https://www.securitylab.ru/blog/personal/Technolady/355083.php>.
3. Проблема борьбы с преступлениями в интернет-пространстве на примере даркнета | Статья в журнале «Молодой ученый» // URL: <https://moluch.ru/archive/340/76332/>.
4. Захаров Н. Д. Понятие и особенности оперативно-разыскной характеристики преступлений против половой неприкосновенности несовершеннолетних, совершенных с использованием сети Интернет // Вестник Волгоградской академии МВД России. 2021. № 3 (58). URL: <https://cyberleninka.ru/article/n/ponyatie-i-osobennosti-operativno-razysknoy-harakteristiki-prestupleniy-protiv-polovoy-neprikosnovennosti-nesovershennoletnih>.
5. Жмуров Д. В. Даркнет как ускользающая сфера правового регулирования // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1 (27). URL: <https://cyberleninka.ru/article/n/darknet-kak-uskolzayuschaya-sfera-pravovogo-regulirovaniya-1>.
6. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное

пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

7. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Широбокова А. А.¹,
студентка группы БЮР202
НИУ «Высшая школа экономики»

Научный руководитель:
Пушкарёв В. В.,
доцент департамента
уголовного права, процесса и криминалистики
НИУ «Высшая школа экономики»,
кандидат юридических наук, доцент

НАЛОГООБЛОЖЕНИЕ КРИПТОВАЛЮТЫ: ПРОБЛЕМНЫЕ ВОПРОСЫ И ПУТИ ИХ РЕШЕНИЯ

В Российской Федерации криптовалюты, несмотря на их широкое распространение, остаются недостаточно урегулированным объектом с точки зрения налогообложения, что создает значительные сложности как для налогоплательщиков, так и для налоговых органов. Настоящая работа посвящена анализу ключевых проблем налогообложения криптовалют в РФ и разработке предложений по их решению.

Одной из ключевых проблем налогообложения криптовалют в РФ является отсутствие четкого правового статуса данного актива, ведь криптовалюта не подпадает под определение «денег» или законного средства платежа в соответствии со ст. 140 Гражданского кодекса РФ и ст. 29 Федерального закона от 10.06.2002 № 86-ФЗ «О Центральном Банке Российской Федерации». Вместе с тем судебная практика, в частности определение Верховного Суда РФ от 02.02.2021 № 44-КГ20-17-К7, признает криптовалюту имуществом в смысле ст. 128 ГК РФ. Это создает правовую неопределенность: с одной стороны, криптовалюта не является законным средством платежа, с другой – рассматривается как объект налогообложения, что подтверждается письмом ФНС России от 04.06.2018 № БС-4-11/10685 [1].

Отсутствие единообразного подхода к правовой природе криптовалюты и с криптовалютой могут возникать как в виде самой криптовалюты, допустим, при майнинге, так и в виде разницы между ценой покупки и продажи на бирже. Однако высокая волатильность криптовалют, подчеркиваемая авторами, затрудняет точную оценку их рыночной стоимости на момент сделки, что может привести к спорам между налогоплательщиками и налоговыми органами [2]. С 01.11.2024 в РФ законодательно легализован майнинг криптовалют (Федеральный закон от 31.07.2020 № 259-ФЗ, ст.ст. 14.2, 14.3). Введены реестры лиц, осуществляющих майнинг, и операторов майнинговой инфраструктуры, ведение которых поручено ФНС России через сервис «МайнингРеестр». Однако, как указывают Васильева и Фрик [3], остаются нерешенными вопросы налогообложения доходов от майнинга. Например, доходы, полученные в виде криптовалюты при майнинге,

¹ © Широбокова А. А., 2025.

должны учитываться по рыночной стоимости на момент их получения, но порядок определения этой стоимости законодательно не конкретизирован [4]. Это создает риск субъективного подхода со стороны налоговых органов и потенциальных налоговых споров. Традиционные системы налогообложения, разработанные для фиатных валют, не учитывают специфику криптовалют, включая анонимность транзакций и отсутствие единого глобального регулятора [5]. Криптовбиржи, избегающие применения КУС («Знай своего клиента») процедур, создают возможности для уклонения от уплаты налогов пользователей своих же платформ, что подтверждается международным опытом, где налоговые органы сталкиваются с трудностями отслеживания таких транзакций [6], отправленных через миксеры или децентрализованных биржи без единой системы контроля (так называемые DEX). В России эта проблема усугубляется отсутствием обязательного декларирования операций с криптовалютами для физических лиц, что снижает прозрачность налогового учета. Кроме того, законопроект Минфина РФ № 1065710-7, одобренный в 2024 г. [7], предусматривает с 2025 г. официальное признание криптовалюты имуществом и введение налоговых ставок: 13 % (или 15 % при доходе свыше 2,4 млн рублей в год) для физических лиц и 20 % для организаций. Однако непроработанность детализированных методик расчета налоговой базы, особенно в условиях волатильности, создает неопределенность для налогоплательщиков [8].

На основе внешнеуровневого анализа проблем, можно предложить следующие меры по совершенствованию налогообложения криптовалют в РФ:

1. Уточнение правового статуса криптовалюты.

Видится важным внести изменения в Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» [9], четко определив криптовалюту как цифровой финансовый актив, обладающий свойствами имущества, но не являющийся законным средством платежа. Это позволит устранить правовую лакуну и создать основу для единообразного налогообложения.

2. Разработка методик оценки рыночной стоимости.

Для учета волатильности криптовалют предлагается установить единый порядок определения их рыночной стоимости на момент совершения операций. Например, можно использовать средневзвешенную цену на ведущих криптовалютных биржах, зарегистрированных в РФ, как это практикуется в некоторых странах, как например, в США IRS использует данные крупных бирж для оценки.

3. Упрощение налогообложения майнинга.

Для доходов от майнинга целесообразно ввести упрощенный порядок декларирования, обязав майнеров предоставлять данные о добытой криптовалюте через реестр ФНС. Также следует разработать нормативные акты, конкретизирующие порядок учета затрат на майнинг, в том числе электроэнергию и оборудование для расчета налоговой базы.

4. Повышение прозрачности операций.

Введение обязательного декларирования операций с криптовалютами для физических лиц, аналогичного декларированию доходов от продажи имущества, позволит повысить контроль со стороны налоговых органов. При этом можно

внедрить цифровые инструменты, такие как интеграция данных с криптовалютных бирж, как это реализовано в Южной Корее [10].

В заключение, отмечается, что проведенное исследование проблем налогообложения криптовалют в Российской Федерации выявило ряд системных противоречий, препятствующих эффективной интеграции цифровых активов в налоговую систему. Отсутствие четкого правового статуса криптовалюты, сложности оценки их рыночной стоимости в условиях высокой волатильности, а также недостаточная прозрачность операций создают вызовы как для налогоплательщиков, так и для налоговых органов. Эти проблемы усугубляются анонимностью транзакций, которая, с одной стороны, является ключевой характеристикой криптовалют, обеспечивающей свободу финансовой деятельности, а с другой – затрудняет контроль за соблюдением налогового законодательства и предотвращение финансовых преступлений, таких как уклонение от уплаты налогов.

Анализ текущего законодательства и правоприменительной практики, включая судебные решения и инициативы Минфина России, показывает, что регулирование криптовалютного рынка в России находится на стадии активного развития. Однако для достижения баланса между обеспечением прозрачности операций и сохранением привлекательности цифровых активов для добросовестных пользователей необходимы дальнейшие шаги. Предложенные меры, такие как уточнение правового статуса криптовалюты, разработка единых методик оценки налоговой базы, упрощение налогообложения майнинга и внедрение обязательного декларирования операций, позволят устранить существующие пробелы в законодательстве. Важно, чтобы эти меры соответствовали принципам соразмерности и технологической нейтральности, не ограничивая права пользователей и способствуя развитию цифровой экономики.

В условиях глобализации финансовых рынков и роста трансграничных операций с криптовалютами особое значение приобретает гармонизация российского законодательства с международными стандартами. Это позволит не только повысить эффективность налогового контроля, но и укрепить позиции России в глобальной криптовалютной экосистеме, обеспечив защиту интересов государства и граждан.

Список литературы

1. Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ // СПС «Консультант Плюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_5142/.
2. Информация Федеральной налоговой службы от 1 ноября 2024 г. «На сайте ФНС России размещен сервис «МайнингРеестр» // ЭПС «Система ГАРАНТ».
3. Определение Судебной коллегии по гражданским делам Верховного суда РФ от 02.02.2021 № 44-КГ20-17-К7, 2-2886/2019 // URL: <https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-grazhdanskim-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-02022021-n-44-kg20-17-k7-2-28862019/>.
4. Письмо ФНС России от 04.06.2018 № БС-4-11/10685@ «О порядке налогообложения доходов физических лиц» // СПС «Гарант».

5. Постановление Правительства РФ от 01.11.2024 № 1468 «Об утверждении Правил установления запрета на осуществление майнинга цифровой валюты (в том числе участие в майнинг-пуле) в отдельных субъектах Российской Федерации или на отдельных их территориях» // Официальный интернет-портал правовой информации. – URL: <http://publication.pravo.gov.ru/document/0001202411010030>.

6. Постановление Правительства РФ от 31.10.2024 № 1464 «Об утверждении Правил ведения реестра лиц, осуществляющих майнинг цифровой валюты, и Правил ведения реестра операторов майнинг-инфраструктуры» // Официальный интернет-портал правовой информации. – URL: <http://publication.pravo.gov.ru/document/0001202411010038>.

7. Пресс-центр Минфина РФ. – URL: https://minfin.gov.ru/ru/press-center/?id_4=39448-vneseny_popravki_v_zakonoproekt_o_maininge_reguliruyushchie_nalogooblozhenie_kriptovalyuty.

8. Федеральный закон от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. – URL: <http://publication.pravo.gov.ru/document/0001202408080016>.

9. Федеральный закон от 10.06.2002 № 86-ФЗ «О Центральном Банке Российской Федерации (Банке России)» // Официальный интернет-портал правовой информации. – URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102077052>.

10. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. – URL: <http://publication.pravo.gov.ru/Document/View/0001202007310056>.

11. Абульханова М. С. Кимчи премиум как основная проблема рынка криптовалют республики корея // Корееведение в России: направление и развитие. 2023. № 2. URL: <https://cyberleninka.ru/article/n/kimchi-premium-kak-osnovnaya-problema-rynka-kriptovalyut-respubliki-koreya> (дата обращения: 11.04.2025).

12. Бакиева М. Ю., Гуреева О. В. Финансовые инновации в российской экономике // Вестник Саратовского государственного социально-экономического университета. 2018. № 3 (72). С. 16–19.

13. Васильева Е. Г., Фрик Д. М. Проблемы и перспективы налогообложения цифровых валют в РФ // International Journal of Humanities and Natural Sciences. – 2024. – № 12-1 (99). – С. 47–52.

14. Кириллова О. С. Налоговые детерминанты развития экономики в современных условиях // Вестник Саратовского государственного социально-экономического университета. 2015. № 2 (56). С. 73–77.

15. Коваленко Е. Г. Проблемы и перспективы налогообложения доходов, полученных от операций с криптовалютой // Вестник Хабаровского государственного университета экономики и права. – 2018. – №2. – С. 67–70.

16. Мазо М. А. Особенности правового содержания принципа свободного перемещения финансовых средств в Российской Федерации // Бизнес в законе. – 2008. – № 1. – С. 60–61.

17. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

18. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

Янгулбаев Х. Х-Б.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:

Михайленко Н. В.,

*доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ОТВЕТСТВЕННОСТЬ ЗА КИБЕРПРЕСТУПЛЕНИЕ В УГОЛОВНОМ КОДЕКСЕ РОССИЙСКОЙ ФЕДЕРАЦИИ: АНАЛИТИЧЕСКИЙ ОБЗОР И СУДЕБНАЯ ПРАКТИКА

Развитие информационных технологий и широкое внедрение Интернета в повседневную жизнь привели к возникновению новых видов правонарушений – киберпреступлений. В связи с этим возрастает актуальность вопрос ответственности за преступления в сфере компьютерных и информационных технологий. Российский уголовный закон был адаптирован с учетом современных реалий, однако его роль и эффективность в обеспечении ответственности за киберпреступления продолжают вызывать профессиональные дискуссии. В статье рассматривается правовая регламентация ответственности за киберпреступления в Уголовном кодексе РФ, анализируются судебные практики, а также выделяются особенности и перспективы совершенствования законодательства в данной сфере.

I. Общие положения о киберпреступлениях в российском законодательстве.

Киберпреступления – это преступные деяния, совершаемые с использованием информационных технологий, в частности, компьютерных систем, сетей и программных средств (ст. 272 Уголовного кодекса РФ). В отечественной юридической практике они рассматриваются как отдельная категория преступлений, требующая специфического подхода к квалификации и ответственности.

Основными нормативными правовыми актами, регулирующими ответственность за киберпреступления, являются:

1. Уголовный кодекс РФ (далее – УК РФ).
 2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
 3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- II. Статьи УК РФ, регулирующие ответственность за киберпреступления.
Наиболее значимыми статьями УК РФ в сфере киберпреступлений являются:

¹ © Янгулбаев Х. Х-Б., 2025.

1. Статья 272. Незаконный доступ к компьютерной информации - предусматривает ответственность за несанкционированный вход в информационную систему, доступ к ее защищенным данным с целью извлечения, уничтожения, изменения или распространения. Наказание – штраф, исправительные работы, ограничение свободы или лишение свободы на срок до 4 лет.

2. Статья 273. Создание, использование и распространение вредоносных компьютерных программ – регулирует ответственность за создание, запуск, распространение вредоносных программ. Наказание до 5 лет лишения свободы.

3. Статья 274. Нарушение правил эксплуатации средств вычислительной техники, автоматизированных систем, их защита – предусматривает ответственность за нарушения, угрожающие безопасности автоматизированных систем, с возможностью штрафов и лишения свободы.

4. Статья 187. Незаконные опечатывание, уничтожение или повреждение электронных носителей информации – регламентирует ответственность за уничтожение или повреждение электронных носителей.

5. Статья 159. Мошенничество – применяется в случаях использования киберметодов для злоупотребления доверием либо получения незаконной выгоды.

Анализ судебной практики.

Практика судов по делам о киберпреступлениях свидетельствует о растущей ответственности государства за пресечение и наказание за использование информационных технологий в противоправных целях.

Примеры судебных решений:

1. Дело о несанкционированном доступе (2018) – суд признал виновным злоумышленника по ст. 272 УК РФ за проникновение в корпоративные системы с целью хищения данных. Назначено наказание в виде 3 лет лишения свободы.

2. Дело о распространении вредоносных программ (2019) – лицо было осуждено по ст. 273 УК РФ за создание и распространение вирусов, обеспечивших кражу средств с банковских счетов. Назначено 4,5 года лишения свободы.

3. Дело о мошенничестве с использованием сети Интернет (2020) – обвиняемый получил крупную сумму путем обмана жертвы, используя поддельные сайты и электронные платежи. Суд приговорил его к 6 годам лишения свободы.

Общий вывод – суды последовательно применяют статьи УК РФ, усиливая ответственность за киберпреступления, и закрепляя тенденцию к их усиленной криминализационной характеристике.

Особенностями ответственности в сфере информационной безопасности являются:

1. Акцент на квалификацию действий по обстоятельствам (например, квалификация по ст.ст. 272 или 273 УК РФ в зависимости от характера преступных деяний).

2. Использование технических средств доказательства – логов, киберэкспертиз.

3. Возможность привлечения к ответственности как физических лиц, так и юридических лиц (ст. 14.1. КоАП РФ за административные правонарушения).

4. Применение дополнительных санкций в виде блокировки сайтов, ограничений в использовании информационных технологий.

Перспективы развития законодательства.

Проблемные аспекты, требующие совершенствования, включают:

1. Недостаточную регламентацию ответственности за использование данных без согласия обладателей, что требует расширения статей, связанных с персональными данными (ст. 137 УК РФ – нарушение неприкосновенности частной жизни).

2. Необходимость более четкого определения критериев квалификации киберпреступлений.

3. Внедрение новых статей, регулирующих ответственность за кибератаку, кибершпионаж и кибертерроризм, что реализуется посредством проекта нового Уголовного кодекса.

Некоторые инициативы уже представлены в законопроектной деятельности, включая Законопроект № 959340-7 «О внесении изменений в УК РФ о ответственности за киберпреступления», что свидетельствует о дальнейшем расширении ответственности.

Заключение.

Ответственность за киберпреступления в РФ закреплена в Уголовном кодексе и дополнена специализированными нормативными актами. Судебная практика демонстрирует растущее внимание судов к этим делам и налагает строгие санкции для преступников, использующих информационные технологии. Однако, с учетом быстрого развития технологий и методов совершения преступлений, необходимо постоянное совершенствование законодательства, расширение статей, укрепление технической базы судебных экспертиз и межведомственного взаимодействия. Это обеспечит более эффективную борьбу с киберпреступностью и повысит уровень ответственности за преступные деяния в цифровой сфере.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025). – Текст: электронный // КонсультантПлюс: [сайт]. – 2025. – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 01.04.2022).

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). – Текст: электронный // КонсультантПлюс: [сайт]. – 2025. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/.

3. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). – Текст: электронный // КонсультантПлюс: [сайт]. – 2025. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.

4. Репьева А. М. Противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий: учебное пособие / А. М. Репьева, В. В. Пушкарев, А. В. Константинов, А. А. Котова – Москва: Изд-во Юридического института РУТ (МИИТ), 2025 – 104 с.

5. Константинов А. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы / А. В. Константинов, Н. В. Михайленко // Вестник Московского университета МВД России. – 2023. – № 3. – С. 129–132.

РАЗДЕЛ IV. ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БОРЬБЕ С ПРЕСТУПНОСТЬЮ В РОССИИ И ЗАРУБЕЖНЫХ СТРАНАХ

Буравлева А. К.¹,

заместитель заведующего кафедрой

иностранных языков Московского университета

МВД России имени В.Я. Кикотя

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ: СРАВНЕНИЕ ЗАКОНОВ О КИБЕРПРЕСТУПНОСТИ В САУДОВСКОЙ АРАВИИ И США

Киберпреступность – это преступление, совершаемое через Интернет с использованием компьютера и сети. Киберпреступность включает в себя широкий спектр незаконных действий, таких как кража данных, нарушение авторских прав, кража личных данных и т.д. распространение компьютерных вирусов и вредоносных программ, мошенничество и многие другие виды преступной деятельности [4]. Данный вид преступлений растет в геометрической прогрессии благодаря постоянному развитию компьютерных технологий и мобильных телефонов. Преступникам стало проще осуществлять кибератаки, когда большинство частных лиц и компаний перешли на онлайн-транзакции [1]. По словам исследователя Серебряковой О. М., «интернет все чаще становится платформой для онлайн-хищников» [9]. С увеличением онлайн-трафика возросла вероятность незаконной деятельности. Преступники разрабатывают новые методы совершения своих преступлений, используя Интернет и современные технологии. Киберпространство злоумышленников нелегко идентифицировать, поскольку они могут быть любого возраста и национальности. Это могут быть отдельные лица, организованные группы или целые государства. Жертвами киберпреступлений становятся пользователи Интернета разных возрастов и национальностей, это могут быть отдельные лица, организации и правительства [2]. Киберпреступность – растущая угроза, затрагивающая цифровой мир и всех, кто им пользуется. Борьба с киберпреступностью стала общей целью для многих стран мира, направленной на предотвращение нарушений информационной безопасности [4].

В настоящее время количество совершаемых киберпреступлений значительно увеличилось, а также произошло расширение спектра типов киберпреступлений: от отдельных случаев взлома с целью развлечения до кибератак, организованных преступными группами, обладающими навыками и опытом для их проведения.

Не во всех странах сегодня существуют законы, связанные с борьбой с киберпреступностью, не каждое государство рассматривает возможность привлечения правоохранительных органов к раскрытию данного вида правонарушений, что дает возможность многим преступникам осуществлять кибератаки из данных

¹ © Буравлева А. К., 2025.

стран [8]. Киберпреступность стала бизнесом, который использует технологии для совершения эффективных и беспрецедентных преступлений. Масштабы и последствия этих преступлений огромны и не могут быть достигнуты в реальном мире.

Соединенные Штаты и Саудовская Аравия относятся к числу стран, где действуют законы о киберпреступности и предусмотрены наказания за нее, однако, чтобы быть более эффективными в более широком масштабе, законы о киберпреступности должны применяться во всем мире [8].

В Соединенных Штатах зарегистрировано множество случаев киберпреступлений, которые затрагивают бизнес и даже правительство. Ниже приведены случаи киберпреступлений, считающиеся наиболее серьезными в США. В октябре 2014 г. Белый дом подвергся кибератаке. Федеральное бюро расследований и другие разведывательные службы США осуществляли расследование данного преступления. Правоохранительными органами считалось, что российское правительство наняло злоумышленников для осуществления данной серьезной кибератаки на правительство США, но подобного рода информация не была подтверждена [6]. В ноябре 2013 г. была осуществлена атака на американскую розничную корпорацию, которая управляет сетью дисконтных универмагов и гипермаркетов, Target Corporation, целью которой стали номера кредитных и дебетовых карт клиентов и другая конфиденциальная информация. Хакеры смогли получить эту информацию и незаметно загрузить данные 110 миллионов клиентов на внешний сервер [5]. Атака на Google, была инициирована в июне 2009 г. и совершена китайской корпорацией Elder wood Gang, специализирующейся на кибершпионаже. Злоумышленники получили доступ к хранилищам исходного кода Google, используя сложную технику, и смогли незаметно извлечь конфиденциальные данные о бизнесе Google [5]. Атака на редакцию New York Times в октябре 2012 г. была совершена с использованием методов, используемых китайскими военными. Целью хакеров были данные сотрудников и репортеров New York Times, а также их пароли. Одной из задач киберпреступников было получение имен тех, кто помогал достать информацию о родственниках премьер-министра Китая. Соответственно, данные 50 сотрудников и журналистов были загружены на внешний сервер [5]. Нападение на американскую многонациональную корпорацию по продаже недорогих универмагов TJX в мае 2006 г. было совершено неизвестной преступной группой, которая смогла получить номера кредитных и дебетовых карт более чем 94 миллионов клиентов. Хакеры смогли загрузить эту информацию на внешний сервер и не были обнаружены [5].

Саудовская Аравия также стала мишенью хакеров, и одними из самых страшных кибератак в данной стране являются следующие преступления. Атака на компанию Agamco, одну из известных нефтяных компаний, принадлежащих правительству Саудовской Аравии, в августе 2012 г. В результате этого инцидента 30 000 компьютеров в компании были атакованы вирусом, что привело к уничтожению данных с жестких дисков компании. Считалось, что целью атаки является прекращение добычи нефти в компании [3]. Многочисленные атаки из-за рубежа были нацелены на правительственные веб-сайты Саудовской Аравии, которые

довольно долго выводили из строя веб-сайты, пока они не были отключены полностью [3]. Было заявлено, что кибератаки были совершены с сотен IP-адресов из разных уголков мира [7]. В 2012 г. было совершено нападение на государственный Университет короля Сауда, расположенный в Эр-Рияде. В результате атаки была взломана база данных университета, в которую входили 812 пользователей. Данные, включающие номера телефонов, адреса и пароли, были взломаны с веб-сайта университета и опубликованы в Интернете на сайте обмена файлами [3]. В мае 2013 г. хакеры атаковали компьютеры национальной полиции Саудовской Аравии, что привело к их сбою после принятия огромного количества запросов на обслуживание [3]. Кроме того, в мае 2013 г. веб-сайт газеты Financial Times и лента Twitter в Саудовской Аравии подверглись кибератакам, предположительно, со стороны группы активистов, поддерживающих президента Сирии и его армию [3].

Соединенные Штаты и Саудовская Аравия – две страны, которые признали важность принятия законов для борьбы с глобальной киберпреступностью и наказания виновных в ее совершении. Экономические издержки киберпреступности как в Соединенных Штатах, так и в Саудовской Аравии ошеломляют. В 2014 г. было подсчитано, что киберпреступность обошлась Соединенным Штатам примерно в 100 миллиардов долларов в год. Расходы на киберпреступность в Саудовской Аравии превышают 1,9 миллиарда долларов в год. И в Соединенных Штатах, и в Саудовской Аравии действуют собственные законы о борьбе с киберпреступностью, касающиеся наиболее распространенных преступлений в каждой стране.

В Соединенных Штатах Закон о компьютерном мошенничестве и злоупотреблениях (CFAA) был принят Конгрессом в 1986 году в качестве отдельного нового закона, 18 U.S.C. § 1030, направленного на борьбу с преступлениями, связанными с использованием компьютеров. Конгресс продолжал пересматривать федеральные уголовные законы и вносить соответствующие поправки для борьбы с растущими преступлениями, связанными с использованием компьютеров и Интернета. Примерами таких поправок являются изменение, внесенное в § 1030 (a)(2)(C) статьи 18 Кодекса США, направленное на устранение концепции, согласно которой кража информации включает в себя «межгосударственное или зарубежное общение, что расширяет юрисдикцию для дел, связанных с кражей информации с компьютеров», а также изменение, внесенное в § 1030(a)(5) статьи 18 Кодекса США, исключающее из закона пункт, согласно которому тяжким преступлением считаются только действия обвиняемого, приводящие к убыткам, превышающим 5000 долларов.

Саудовская Аравия – исламское государство, основывающее свою правовую и судебную систему на принципах исламского права (шариата). Исламское право используется как в гражданских, так и в уголовных делах. Король Саудовской Аравии является главой правовой системы и представляет апелляционный суд последней инстанции, в его руках находится право на помилование.

Саудовская Аравия является страной, наиболее подверженной киберпреступности в регионе Персидского залива. В стране действует собственный закон о

борьбе с киберпреступностью, который предусматривает наказание нарушителей в киберпространстве. В марте 2007 г. в Саудовской Аравии был принят Закон о борьбе с киберпреступностью, который определяет несанкционированный доступ как преднамеренный, несанкционированный доступ любого лица к компьютерам, веб-сайтам, информационным системам и компьютерным сетям. Этот закон определяет определенные киберпреступления и определяет меры наказания за них. Слежка, перехват или получение данных, передаваемых через информационную сеть или компьютер без законного разрешения, является киберпреступлением (статья 3(1)) Закона о борьбе с киберпреступностью. Статья 3 предусматривает наказание за это преступление в виде «тюремного заключения на срок не менее одного года и штрафа в размере до пятисот тысяч долларов (Саудовских риалов)». Взлом веб-сайта с намерением изменить его дизайн, уничтожить, модифицировать или занять его URL-адрес является киберпреступлением (статья 3(3)). Статья 3 предусматривает наказание в виде «тюремного заключения на срок не менее одного года и штрафа в размере не более пятисот тысяч саудовских риалов или любого другого вида наказания». Киберпреступлением является остановка работы информационной сети или уничтожение, утечка или изменение существующих программ или данных (статья 5(2)). Статья 5 предусматривает наказание за это преступление в виде «тюремного заключения на срок до четырех лет и штрафа в размере до трех миллионов саудовских риалов или любого другого вида наказания». Незаконный доступ к информационной системе с целью получения данных, которые могут поставить под угрозу внутреннюю или внешнюю безопасность государства или его национальную экономику, является киберпреступлением (статья 7(2)). Статья 7 предусматривает наказание за это киберпреступление в виде «тюремного заключения на срок до десяти лет и штрафа в размере до пяти миллионов риалов или любого другого вида наказания». Незаконный доступ к компьютерам с намерением угрожать или шантажировать любое лицо, чтобы заставить его предпринять какие-либо действия или воздержаться от них, является киберпреступлением (статья 3(2)). Статья 3 предусматривает наказание за это преступление в виде «тюремного заключения на срок не менее одного года и штрафа в размере до пятисот тысяч долларов. Саудовские риалы или любое другое наказание». Производство, подготовка, передача или хранение электронных материалов, которые оказывают негативное воздействие на общественный порядок и общественную мораль, являются киберпреступлением (статья 6(1)). Создание любого веб-сайта, пропагандирующего или облегчающего торговлю людьми, является киберпреступлением (статья 6(2)). Подготовка, публикация и продвижение материалов для порнографических сайтов или сайтов азартных игр, нарушающих общественную мораль, является киберпреступлением (статья 6(3)). Создание любого веб-сайта, который демонстрирует методы употребления наркотических средств или психотропных веществ, или облегчает торговлю ими, признается киберпреступлением (статья 6(4)). Статья 6 определяет наказание за эти преступления как «тюремное заключение на срок до пяти лет и штраф в размере до трех миллионов риалов или любое другое наказание».

Таким образом, в США и Саудовской Аравии существует ряд законов, которые направлены на предотвращение преступлений, связанных с информационно-телекоммуникационными технологиями. Данный вид преступлений наносит значительный вред странам, поэтому в определенный момент возникла необходимость в создании законов, которые будут защищать физические и юридические лица обеих стран от данных преступлений. Обе страны серьезно подошли к вопросу создания и реализации законодательной базы против киберпреступлений, что, несомненно, привело к видимым результатам в виде снижения уровня киберпреступности на территориях данных стран.

Список литературы

1. Broadhurst R. Developments in the global law enforcement of cyber-crime // *Policing*, 2006, № 29(3), pp. 408–433.
2. Desnoyers S. The challenges of cybercrime for international law enforcement (Order No. 1551187). 2013. Available from ProQuest Dissertations & Theses Global. (1498133652).
3. Elnaïm B.M. Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future // *Information and Knowledge Management*, 2013, № 3(12), pp. 14–19.
4. Hu Y., Chen X., Bose, I. Cybercrime enforcement around the globe // *Journal of Information Privacy & Security*, 2013, № 9(3), pp. 34–52.
5. Kadivar M. Cyber-attack attributes // *Technology Innovation Management Review*, 2014, № 4(11), pp. 22–27.
6. Perez E., Prokupecz S. How the U.S. thinks Russians hacked the White House. CNN. 2015. URL: <http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/>.
7. Reuters. Saudi Arabia faces major cyber attack. Gulf News. 2013. URL: <http://gulfnews.com/news/gulf/saudi-arabia/saudi-arabia-faces-major-cyber-attack-1.1184977>
8. Thompson L. Defending against cybercrime (Order No. 1570878). 2014. Available from ProQuest Dissertations & Theses Global. (1640916948).
9. Серебрякова О. М. Киберсталкинг и киберзапугивание: последствия и меры профилактики // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий: Международная научно-практическая конференция, 18 апреля 2024 г.: сборник научных трудов / сост. А. В. Константинов. М.: Московский университет МВД России имени В.Я. Кикотя, 2024. С. 529–534.

Воротникова И. Г.¹,
доцент кафедры иностранных языков
Московского университета
МВД России имени В.Я. Кикотя,
кандидат филологических наук, доцент

КИБЕРПРЕСТУПНОСТЬ КАК ГЛОБАЛЬНАЯ ИНДУСТРИЯ И ЕЕ ЭКОНОМИЧЕСКИЕ ПОСЛЕДСТВИЯ

Киберпреступность представляет собой значительную угрозу для любой отрасли и организации. В настоящее время киберпреступность, по данным Всемирного экономического форума (ВЭФ), является третьей по величине экономикой в мире, уступая лишь США и Китаю.

Развитие киберпространства открыло «шлюзы» для притока нового типа преступников. Злоумышленники образуют в цифровом пространстве разветвленную преступную сеть, которую с учетом ее масштабов называют «индустрией» киберпреступности [4].

По мнению американского ученого Нира Кшетри, индустрия киберпреступности носит глобальный и организованный характер, при этом прогнозирование возможных экономических последствий, совершаемых киберпреступлений и веб-атак с достаточной степенью точности является сложной задачей [3].

Исследователи отмечают, что основными «игроками» в глобальной индустрии киберпреступности являются киберпреступники и их жертвы, но есть и другие участники, в частности, государство (и его нормативно-правовая база) и так называемые «системы», которые содействуют (или препятствуют) совершению киберпреступлений [4].

Экспертная оценка Cybersecurity Ventures, известной отраслевой исследовательской и медийной организации, получившей признание благодаря инновационным идеям и вкладу в развитие кибербезопасности, свидетельствует о том, что к 2025 г. в мире будет храниться 200 зеттабайт данных, что эквивалентно одному триллиону гигабайт или 1021 байту [5]. Этот значительный информационный массив представляет огромную ценность и будет оставаться мишенью для киберпреступников.

Злоумышленниками используются пробелы в системе цифровой безопасности, ее уязвимости, нарушения в сфере кибергигиены как отдельных лиц, так и организаций.

Одной из тенденций, оказывающих существенное влияние на рост киберпреступности и тем самым дестабилизирующих мировую экономику, является отсутствие у преступников глубоких технических знаний для проведения кибератак [1].

Исследование, представленное в рамках Всемирного экономического форума (ВЭФ), показало, что основными факторами, способствующими совершению киберпреступлений, являются, например, несанкционированный доступ к сетям и

¹ © Воротникова И. Г., 2025.

вредоносному программному обеспечению, которое по довольно низкой цене приобретается в «темной паутине» или на нелегальных сервисах RaaS (Ransomware-as-a-Service), продающих соответствующие наборы вредоносных киберинструментов, поставляемые даже с гарантиями качества, а также киберстрахование и высокая мотивация киберпреступников в связи с ожидаемой ими материальной выгодой, получаемой подобным преступным путем [1; 2].

Статистические данные свидетельствуют о том, что преступная деятельность в сфере информационно-телекоммуникационных технологий приносит намного больше денег, чем незаконный оборот наркотиков, контрафакт и торговля людьми вместе взятые. Дополнительные доходы индустрии киберпреступности рассчитываются на основе оценочной стоимости повреждения и уничтожения данных, украденных денег, потери уровня производительности, кражи интеллектуальной собственности, кражи личных и финансовых данных, хищений, мошенничества, нарушения деятельности предприятия после атаки, проведения судебной экспертизы, восстановления и удаления взломанных данных и систем, а также ущерба, нанесенного репутации [2].

В связи с этим эксперты отмечают, что современные технологически совершенствующиеся киберпреступления имеют гораздо более серьезные экономические последствия, чем большинство обычных преступлений. Так, например, руководитель отдела криминалистики международной аудиторской и консалтинговой организации PricewaterhouseCoopers (PwC), представляющий данную группу в мире и Великобритании, подчеркивает тот факт, что в то время как распространенность традиционных видов мошенничества, таких как присвоение активов, с 2014 г. заметно снизилась, наблюдается значительный рост числа предприятий и организаций, сообщающих о фиксируемых ими киберпреступлениях, поскольку применяемые во всех сферах современные технологии влияют на рост численности совершаемых в мире экономических преступлений [6].

Согласно данным Глобального обзора экономических преступлений, проводимого раз в два года корпорацией PwC, более 43 % опрошенных компаний сообщили, что пострадали от одного или нескольких значительных экономических преступлений, причем средний ущерб от мошенничества на одну компанию за два года вырос почти на 40 %; доля компаний, столкнувшихся с утечкой данных на сумму более 1 млн долларов, значительно увеличилась за год – с 27 до 36 % [6; 3].

Среди компаний, столкнувшихся с утечкой данных, численность которых увеличилась с момента проведения исследования PwC в 2023 г., больше всего пострадала отрасль здравоохранения. Средняя мировая стоимость наиболее разрушительной кибератаки составила 4,4 млн долларов, в то время как в секторе здравоохранения эта стоимость была на 25 % выше – 5,3 млн долларов. Почти половина (47 %) респондентов из числа организаций здравоохранения сообщили о нарушении системы безопасности данных на сумму 1 млн долларов или более [6].

По данным Центра стратегических и международных исследований (CSIS) и компании McAfee, экономическое воздействие киберпреступности наиболее

сильно выражено в Европе и достигает 0,84 % регионального ВВП, в Северной Америке оно составляет 0,78 % регионального ВВП [1].

Киберпреступность оказывает большое и быстро растущее влияние на предприятия и организации всех типов – от малых предприятий до крупнейших промышленных компаний и корпораций. Даже изначально небольшие кибератаки на компании могут легко выйти из-под контроля и превратиться в мегахатастрофу. Киберпреступникам не обязательно атаковать компанию напрямую, чтобы нанести ей ущерб. Они могут нанести урон бизнесу, атакуя поддерживающую его инфраструктуру, в частности электросети, системы управления воздушным движением и транспортом, а также коммерческие базы данных и информационные системы финансовых учреждений [4]. Это приводит к тому, что преступники с низкими техническими навыками осуществляют сложные кибератаки, традиционно направленные на сферы здравоохранения, образования и бизнеса. Среди подобных кибератак предпочтение отдается использованию брешей в системе безопасности для распространения программ-вымогателей [2].

Считается, что, помимо уже упомянутых сфер, высокому риску кибератак также подвержены критически важные объекты инфраструктуры, включая электрические, газовые и водопроводные сети, телекоммуникации и транспортные услуги. В результате кибератак 60 % организаций прекратили свою деятельность в течение шести месяцев после того, как стали жертвами вредоносного кибервоздействия [2].

Одна хакерская атака или серия кибератак может дорого обойтись бизнесу и экономике. Так, например, в историю киберпреступлений вошли две масштабные хакерские атаки, ставшие всеобщим потрясением.

Атака вируса-вымогателя WannaCry в мае 2017 г. нанесла глобальный ущерб, поскольку вредоносным программным обеспечением были затронуты более 200 тыс. компьютеров в 150 странах, вследствие чего пострадали банки, предприятия и организации по всему миру, включая медицинские учреждения и технологические компании. Вирус-шифровальщик парализовал работу компьютеров и вымогал у пострадавших организаций деньги за предоставление кодов расшифровки, которые, однако, были ложными. По официальным данным, нанесенный ущерб составил один миллиард долларов.

Вслед за WannaCry на компьютерные системы крупных корпораций и государственных органов многих стран обрушился вирус NotPetya («злой младший брат» вируса Petya 2016 г.), который атаковал Windows-системы, зашифровывал файлы и требовал выкуп в биткойнах за их расшифровку. Атака данного вируса обошлась мировой экономике в сумму более 10 миллиардов долларов всего за четыре дня. Для сравнения: годовой доход Microsoft – крупнейшей в мире компании по производству программного обеспечения и одной из самых богатых фирм в мире – в 2022 г. составил около 200 миллиардов долларов. Сегодня киберпреступники, как свидетельствует статистика [1], делят между собой банк, превышающий годовой доход Microsoft более чем в 50 раз.

В 2023 г. объем нанесенного экономике глобального ущерба в результате свершенных киберпреступлений составил 8 триллионов долларов, а к 2025 г., по

оценкам специалистов [1], он может достигнуть 10,5 триллионов долларов, причем большая часть доходов будет приходиться на вредоносные программы ransomware.

По прогнозам, экономика киберпреступности будет постоянно расти из года в год, а субъекты угроз будут эксплуатировать одну и ту же жертву спустя месяцы или годы. В последнее время наблюдается всплеск объединения усилий киберпреступных организаций, что повышает серьезность будущих атак и стратегий нападения [6].

С целью противодействия киберпреступности государственные структуры стали активнее реагировать на атаки вирусов-вымогателей и оказывать поддержку компаниям в процессе их восстановления, что привело к снижению количества выкупов, выплачиваемых пострадавшими компаниями за расшифровку данных. Кроме того, стремясь снизить стоимость последствий кибератак на свои компании, они стали приобретать киберстрахование. Эта дополнительная защита была призвана сократить расходы компаний на ликвидацию последствий атак вирусов-вымогателей [2].

Консалтинговые компании проводят всесторонние исследования глобальных киберугроз, новых тенденций и динамики рынка, предоставляя ценные аналитические материалы, основанные на актуальной статистике [6]. В качестве мер противодействия киберпреступности профессионалы в данной сфере рекомендуют предприятиям минимизировать возможности для совершения экономических преступлений путем тщательной оценки рисков мошенничества, подкрепленной культурой, основанной на общих корпоративных ценностях, надежной политике и соблюдении программных требований кибербезопасности.

Список литературы

1. Chin K. The Impact of Cybercrime on the Economy // UpGuard. 05.01.2025. URL: <https://www.upguard.com>.
2. Cybercrime: The World's. 3rd Largest Economy // Critical Start. 2024. URL: <https://www.criticalstart.com>.
4. Kshetri N. The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives. Berlin Heidelberg: Springer-Verlag, 2010. 251 p.
5. Moskowitz S.L. The Global Cybercrime Industry // Cybercrime and Business. 2017. P. 3-22. DOI:10.1016/B978-0-12-800353-4.00500-5.
6. Parekh M. Cybersecurity Ventures Report on Cybercrime // eSentire. 23.07.2024. URL: <https://www.esentire.com>.
7. PwC 2024 Global Digital Trust Insights. PwC. 2024. URL: <https://www.pwc.com>.

Серебрякова О. М.¹,

доцент кафедры иностранных языков

Московского университета МВД России имени В.Я. Кикотя,

кандидат филологических наук

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МЕР ПО ПРЕДОТВРАЩЕНИЮ КИБЕРПРЕСТУПНОСТИ ПОСРЕДСТВОМ МОНИТОРИНГА ГОСУДАРСТВЕННОЙ ПОЛИТИКИ

В Канаде одно из самых последних и всеобъемлющих исследований, проведенных в 2017 г. с репрезентативной выборкой из 10 000 предприятий, показало, что что более чем пятая часть из них пострадала в результате инцидента с кибербезопасностью и что компании всех размеров потратили за предыдущий год 14 миллиардов канадских долларов на системы защиты от различных форм онлайн-угроз [1]. В результате за последние несколько лет киберриски возглавили список проблем безопасности для правительств и бизнес-лидеров, и ожидаются еще более разрушительные последствия, поскольку наши общества становятся все более киберзависимыми и взаимосвязанными. По словам исследователей А. К. Буравлевой и Д. Я. Мушаковой, «быстрое развитие преступлений в сфере информационно-телекоммуникационных технологий заставило правовые системы во всем мире адаптироваться к новым потребностям в защите общества от все более изощренных угроз киберпреступности» [8].

Несмотря на глобальные масштабы и влияние киберпреступности, существует мало инструментов для оценки эффективности политики по снижению уровня киберпреступности. Недавние события в США, Великобритании, Франции и примерно в 40 других странах показали, что киберугрозы могут выходить за рамки критически важных инфраструктур и онлайн-финансовых сервисов и нацеливаться на избирательные процессы и подрывать доверие к демократическим институтам [2]. В ответ на этот быстро меняющийся ландшафт рисков правительства по всему миру разрабатывают политику кибербезопасности и выделяют миллиарды долларов из своих оборонных бюджетов и бюджетов на исследования и разработки на новые программы, которые повысят их способность противостоять киберрискам. Федеральное правительство США, например, в 2019 г. потратило на кибербезопасность почти 16,6 миллиарда долларов [7]. В Великобритании в ноябре 2015 г. канцлер объявил об инвестициях в кибербезопасность в размере 1,9 млрд фунтов стерлингов в течение пяти лет, что позволило увеличить общие обязательства правительства в области кибербезопасности до 3,2 млрд фунтов стерлингов [6]. Австралия, страна со средним уровнем развития, в 2016 г. объявила о разработке всеобъемлющей стратегии кибербезопасности, предусматривающей выделение 230 миллионов австралийских долларов в течение пяти лет [3]. Европейский союз сосредоточил свои инвестиции в кибербезопасность на исследованиях и разработках, планируя финансировать предприятия и университеты. Объем финансирования составит 450 миллионов

¹ © Серебрякова О. М., 2025.

евро в течение четырех лет (с 2017 по 2020 год), при этом ожидается, что сотрудничество государственного и частного секторов позволит привлечь в три раза больше соответствующих средств [4].

Несмотря на эти масштабные инвестиции в политику предотвращения киберпреступности и кибербезопасности, существует очень мало инструментов, которые помогли бы разработчикам политики и общественности определить эффективность государственных мер по борьбе с онлайн-угрозами. Мониторинг политики – это основанный на фактических данных подход, который исследователи государственной политики используют как способ оценки и сравнения эффективности законов. Данный способ основан на систематическом сборе данных о разработке и реализации политики, тщательной оценке ее воздействия и широком распространении этих оценок. Мониторинг политики может способствовать созданию более надежной базы знаний об инициативах по предотвращению киберпреступности, разрабатываемых во всем мире, с целью содействия распространению эффективной политики и предотвращения принятия контрпродуктивных мер.

На международном уровне отсутствие исходной информации ограничивает распространение знаний и препятствует принятию мер политики, которые дают положительные результаты, а также разоблачению неудачных или контрпродуктивных мер политики. Уроки, извлеченные на местном уровне, не распространяются на глобальном уровне, хотя проблемы киберпреступности очень схожи в разных странах, находящихся на сопоставимых этапах экономического и технологического развития. Более устойчивые и систематические усилия по передаче знаний могли бы помочь как зрелым, так и формирующимся цифровым компаниям. экономики пользуются преимуществами более безопасной онлайн-экосистемы. Наконец, отсутствие общей основы для анализа политики предотвращения киберпреступности препятствует координации усилий, которые могли бы обеспечить более эффективное реагирование на транснациональную киберпреступность и киберриски.

В то время как международные организации, такие как Международный Телекоммуникационный союз и Интерпол или европейские агентства, такие как Европол, приступили к разработке амбициозных инициатив по наращиванию потенциала для поддержки развитых и развивающихся стран. В усилиях стран по защите своих граждан от киберпреступлений отсутствие систематических знаний о том, какая политика в каких странах уже реализуется, какой ценой и с какими результатами, сокращает возможности для согласования и синхронизации политики.

Киберпреступность – не единственная область политики, в которой отсутствует интеграция информации, необходимой для содействия осуществлению эффективной или перспективной политики и стратегий вмешательства в различных местных и национальных контекстах.

В настоящее время создано несколько инициатив для обобщения информации – целей, уровня проработанности и, в меньшей степени, результатов – о политике в области предотвращения киберпреступлений и кибербезопасности. Хотя были приложены все усилия для включения всех известных платформ мониторинга

политики в киберпространстве, динамичный характер этой области исследований означает, что некоторые недавние инициативы, возможно, остались незамеченными.

Индекс киберготовности (CRI) был первоначально разработан в 2013 г. Мелиссой Хэтэуэй (бывшим сотрудником администрации Буша и Обамы) для Потомакского института политических исследований (Potomac Institute for Policy Studies) и обновлен в 2015 г. Индекс киберготовности изучает уровень зрелости, который страны демонстрируют в своих усилиях по развитию потенциала в области кибербезопасности [5], и предпринята попытка оценить оперативный потенциал страны по семи измерениям: национальная стратегия, реагирование на инциденты, электронная преступность и правоохранительная деятельность, обмен информацией, инвестиции в исследования и разработки, дипломатия и торговля, а также оборона и антикризисное реагирование. Каждое измерение разбито на четыре компонента: заявление (наличие официальной политики), организация (наличие учреждений, которые могут осуществлять эту политику), ресурсы (распределение финансовых и людских ресурсов, а также создание инструментов измерения для оценки воздействия киберугроз и политики, направленной на их устранение) и внедрение (доказательства эффективности политики). Для оценки каждого аспекта используются три уровня готовности: недостаточная доказательная база (данные отсутствуют или малодоступны), частично работоспособная (результаты наблюдаются, но их функциональность по-прежнему трудно измерить) и полностью работоспособная (функционирующие мероприятия можно наблюдать и измерять). Следует отметить, что показатели, используемые в этой методологии, в большей степени ориентированы на результаты политики или на то, как она реализуется, чем на их результаты или то, к какому эффекту они приводят. По состоянию на апрель 2019 г. команда по обеспечению готовности к киберпространству опубликовала одиннадцать подробных обзоров для Франции, Германии, Индии, Италии, Японии, Марокко, Нидерланды, Саудовская Аравия, Южная Африка, Соединенное Королевство и Соединенные Штаты Америки.

Портал возможностей в области кибербезопасности, поддерживаемый Глобальным центром возможностей в области кибербезопасности в Оксфордском университете, предоставляет общую информацию о национальных и международных инициативах по наращиванию потенциала. Он разработал модель зрелости потенциала стран в области кибербезопасности (СММ), которая оценивает потенциал стран по пяти измерениям: политика и стратегия; культура и общество; образование, профессиональная подготовка и навыки; нормативно-правовая база; стандарты, организации и технологии. Каждое измерение включает в себя подфакторы, которые кажутся исключительно качественными и больше ориентированы на реализацию политики и результаты, чем на конечные результаты. Каждый субфактор оценивается по пятиуровневой шкале (стартап, формирующий, устоявшийся, стратегический и динамичный). Из 24 аспектов и подфакторов, составляющих модель, только один затрагивает проблему киберпреступности, объединяя мероприятия по расследованию и предотвращению в единый компонент. На веб-сайте портала указано, что СММ была внедрена более чем в 100

странах при финансовой поддержке Всемирного банка, Международного союза электросвязи и других международных организаций, но только в четырнадцати подробных обзорах (Албания, Бутан, Кипр, Исландия, Индонезия, Косово, Кыргызстан, Литва, Македония, Мадагаскар, Сенегал, Сьерра-Леоне, Уганда и Великобритания) и региональный отчет, содержащий анализ высокого уровня по 32 странам Латинской Америки и Карибского бассейна, доступны для скачивания.

Информационные панели по кибербезопасности ЕС и Азиатско-Тихоокеанского региона разрабатываются бизнес-группой Software Alliance, представляющей индустрию программного обеспечения. Их цель – оценить степень зрелости политики кибербезопасности в 28 европейских и 10 азиатских странах. Каждая страна оценивается по 25 критериям, в основном относящимся к программам и мероприятиям, сгруппированы по пяти темам: правовые основы, оперативные подразделения, государственно-частное партнерство, отраслевые планы обеспечения кибербезопасности и образование. Каждый критерий оценивается как удовлетворенный, частично удовлетворенный или отсутствующий. Не существует сводного индекса или балльной оценки, а также рейтинга стран. Загружаемые отчеты в формате PDF содержат краткие обзоры стран с дополнительной качественной информацией, освещающей конкретную политику.

Реестр Глобального форума по киберэкспертизе поддерживается Глобальным центром потенциала в области кибербезопасности Оксфордского университета. В нем перечислены и описаны международные программы и инициативы государственных и частных заинтересованных сторон, направленные на повышение кибербезопасности и предотвращение киберпреступности. В базе данных доступен поиск по регионам (Центральная Азия, Европа, Северная Америка и т. д.) и тематике (киберпреступность, кибербезопасность, защита данных, электронное управление). Описания инициатив (обычно состоящие из одного предложения) содержат краткую информацию об организациях-спонсорах, партнерах, целевых странах и группах, целях и задачах, видах проводимых мероприятий, ожидаемых результатах, сроках и контактных данных.

Глобальный индекс кибербезопасности публикуется Международным союзом электросвязи (МСЭ). База данных оценивает возможности 194 стран в области кибербезопасности в пяти измерениях: правовые меры, технические меры, организационные меры, наращивание потенциала и сотрудничество, которые далее разбиты на 25 показателей. МСЭ предельно ясно дает понять, что в ней оценивается приверженность стран на основе предпринимаемых ими действий, а не воздействия, которое их участие оказывает на пользователей, например, повышение уровня защиты. Например, в области киберпреступности основными проблемами Глобального индекса кибербезопасности являются наличие или отсутствие законодательства о киберпреступности и возможностей правоохранительных органов. Эффективность законодательной рамочной программы и инициативы по проведению расследований или обмену информацией не оцениваются. Глобальный индекс кибербезопасности включает как первичные данные, предоставляемые самими странами, так и общедоступные вторичные данные. В результате взвешивания данных получается итоговая оценка страны в диапазоне от 0 до 1,

при этом Великобритания заняла первое место в рейтинге стран в 2018 г. с показателем 0,931 (ITU 2018), заменив Сингапур, чей рейтинг снизился с 0,925 до 0,898 за один год.

База данных International Cyber Developments Review (INCYDER) ведется Совместным центром передового опыта в области киберзащиты NAT. В нем перечислены правовые и политические документы, принятые семнадцатью международными и региональными организациями, такими как ООН, G7, ЕС и т.д. Из-за своей направленности на киберзащиту база данных INCYDER содержит очень мало документов, связанных с киберпреступностью, и в него не включены международные организации по сотрудничеству с полицией, такие как Интерпол или Европол. INCYDER не рассматривает результаты политики и не содержит ссылок на научные публикации, в которых обсуждаются и/или оцениваются эти политики.

Национальный индекс кибербезопасности (NCSI) был запущен в 2016 г. Эстонским управлением электронного управления Academy, при поддержке эстонского правительства и международных партнеров из частного сектора. В рамках этого двухлетнего проекта стоимостью 200 000 евро была разработана методология оценки готовности стран предотвращать киберугрозы, а также их готовности реагировать на кибератаки. Индекс ранжирует 130 стран и основан на 46 показателях, сгруппированных по трем основным категориям (общая кибербезопасность, базовая кибербезопасность и управление инцидентами и кризисными ситуациями) и двенадцати возможностей. Баллы начисляются в зависимости от достигнутого уровня потенциала, а интерактивный инструмент позволяет проводить сравнения между странами 14. Как и во многих других показателях, измеряется наличие конкретных институтов и программ, а не их эффективность – или ее отсутствие – в обеспечении защиты от киберугроз.

Рассмотренные выше платформы используют страны в качестве единицы анализа для получения совокупных оценок. Этот подход поддерживает глобальную передачу политики, но не позволяет исследователям и лицам, принимающим решения, анализировать индивидуальные преимущества или недостатки конкретной политики и программ. В результате такого широкого подхода, ориентированного на конкретные страны, а также из-за нехватки из имеющихся количественных данных о возможностях обеспечения кибербезопасности и их влиянии все платформы мониторинга опираются на качественные данные, полученные из официальных и юридических документов: показатели, полученные в рамках этих инициатив, являются результатом накопления общедоступной информации о существовании или отсутствии ограниченного набора учреждений, программ и практик. Это в значительной степени объясняет, почему, несмотря на заявления о методологиях, основанных на фактических данных, большинство платформ уделяют больше внимания реализации политики и ее результатам, таким как разработка мер в чрезвычайных ситуациях, группы реагирования, механизмы обмена правовой информацией, государственно-частные партнерства или программы повышения осведомленности – и в меньшей степени о результатах этих

мер политики, которые потребовали бы жестких показателей, таких как сделанные инвестиции, зарегистрированный уровень заражения или количество пользователей, защищенных от различного вреда.

Список литературы

1. Bilodeau H., Lari M., Uhrbach M. Cyber Security and Cybercrime Challenges of Canadian Businesses. Ottawa: Statistics Canada, 2017.
2. CSE. 2017. Cyber Threats to Canada's Democratic Process. Ottawa: Communications Security Establishment.
3. Duckett C. Budget 2016: Australian Cyber Strategy Implementation Broken Out. ZDNet. 2016. URL: <http://www.zdnet.com/article/budget-2016-australian-cyber-strategy-implementation-broken-out/>.
4. European Commission. 2016. Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats. URL: http://europa.eu/rapid/press-release_IP-16-2321_en.htm.
5. Hathaway M., Demchak C., Kerben J., McArdle J., Spidalieri F. Cyber Readiness Index 2.0 - A Plan for Cyber Readiness: A Baseline and an Index. Washington DC: Potomac Institute for Policy Studies, 2015.
6. Osborne, G. 2015. Chancellor's Speech to GCHQ on Cyber Security. URL: <https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security>.
7. The White House. 2019. Cybersecurity Funding. URL: https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf.
8. Буравлева А. К., Мушакова Д. Я. Эволюция законодательства о киберпреступности в контексте правового развития цифрового мира // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Международная научно-практическая конференция, 18 апреля 2024 г. : сборник научных трудов / сост. А. В. Константинов. М.: Московский университет МВД России имени В.Я. Кикотя, 2024. С. 473–476.

Вачаев В. В.¹,

курсант 533 учебного взвода 2 курса

международно-правового факультета

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Алексич Е. В.,

доцент кафедры иностранных языков

Московского университета МВД России

имени В.Я. Кикотя,

кандидат педагогических наук

СОТРУДНИЧЕСТВО ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ СТРАН США И ВЕЛИКОБРИТАНИИ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ НА ПРИМЕРЕ МЕГАПОЛИСОВ

В наше время, когда цифровые технологии играют ключевую роль в жизни человека, киберпреступность приобретает статус одной из наиболее значимых угроз безопасности общества. Особенно в мегаполисах – местах сосредоточения основных ресурсов. А при условиях глобализации преступные группы используют современные технологии для совершения атак, что обуславливает необходимость международного сотрудничества при борьбе с киберугрозами. Так, США и Великобритания, являясь одними из ведущих мировых держав, обладают богатыми опытом и ресурсами в области кибербезопасности, что делает их взаимодействие в данной сфере очень важным.

Исторически предпосылки к сотрудничеству правоохранительных органов США и Великобритании исходят из середины XX в., а точнее в 1946 г., когда состоялось подписание соглашения UKUSA, которое заложило фундамент для обмена разведданными между этими странами. Положения, закрепленные в этом соглашении, были направлены на укрепление безопасности в условиях послевоенного мира и способствовали укреплению доверия и взаимопонимания между странами. Со временем сотрудничество стран охватывало все новые сферы, в том числе и борьбу с киберпреступностью, что с необычайно быстрым развитием технологий стало актуально. Что касается юридического аспекта взаимодействия правоохранительных органов США и Великобритании, его составляет ряд международных соглашений. Так, можно выделить соглашение о взаимной правовой помощи, которое было подписано в 2001 г. и является одним из ключевых. Это соглашение определяет вопросы сотрудничества в области противодействия киберпреступлениям, в том числе обмен информацией, проведение совместных расследований, а также оказание правовой помощи в рамках международного права. Подобные правовые механизмы составляют основу эффективного взаимодействия и координации действий стран в борьбе с киберугрозами.

¹ © Вачаев В. В., 2025.

Итак, оба этих аспекта сотрудничества США и Великобританией оказали значительное влияние на борьбу с киберпреступностью. Доверие, сложившееся исторически на основе длительного взаимодействия, и юридические механизмы, выражающиеся в соглашениях, образуют условия для эффективного противодействия киберугрозам. С 2014 г. в рамках Форума по вопросам кибербезопасности, правоохранительные органы обеих стран проводят совместные учения и мероприятия, которые способствуют совершенствованию навыков и обмену опытом, что наглядно показывает, как исторические и юридические основы способствуют укреплению безопасности в нынешних условиях.

Совместные операции, которые проводятся правоохранительными органами США и Великобритании в мегаполисах, представляют собой сложный процесс, который включает в себя как координацию действий, обмен информацией, так и использование специально разработанных технологий. Эти операции, направлены на борьбу с киберпреступлениями, что делает их актуальными в условиях больших городов, ведь именно в таких местах концентрация потенциальных целей высока. Ключевым элементом таких операций является использование ресурсов обоих государств, включая аналитические центры, экспертов в области кибербезопасности и передовые средства мониторинга. Это позволяет правоохранительным органам обеих стран эффективно противостоять угрозам, исходящим от организованных кибергруппировок. При этом сохраняются проблемы, связанные с коррупцией в правоохранительных органах. Например, согласно отчету, «полиция была наиболее часто упоминаемой организацией, получившей взятки» (Sagat, Shaw, 2010. 44 с.). Это свидетельствует о необходимости постоянного контроля и повышения прозрачности в работе правоохранительных структур, что является важным аспектом для успешного выполнения совместных операций.

Одним из ярких примеров успешного сотрудничества является операция против хакерской группы REvil, проведенная в 2020 г. Так, рассматривая кибератаки, нельзя не затронуть последствия, которые они оказывают на мегаполисы, такие как Нью-Йорк и Лондон, выходя за рамки непосредственного ущерба. Атака на метро Нью-Йорка в 2017 г. продемонстрировала уязвимость транспортной инфраструктуры, что может негативно сказаться на экономической активности и снизить доверие к ее надежности. Аналогично атака на NHS в Лондоне в 2021 г. не только привела к утечке данных, но и подорвала доверие граждан к системе здравоохранения. Эти инциденты подчеркивают необходимость усиления кибербезопасности в мегаполисах, особенно с учетом того, что «сложность мегаполисов представляет собой уязвимую и сложную оперативную среду будущего» (Каун, 2016, с. 3). Учитывая потенциальное влияние кибератак на качество жизни и безопасность граждан, важно рассматривать эту проблему в ее многогранности и принимать меры для ее решения.

Киберпреступность оказывает значительное воздействие на социальную структуру мегаполисов, влияя на экономическое благополучие граждан и общественное доверие. Одним из ключевых последствий является финансовая нестабильность, вызванная утратой персональных данных и финансовых средств. Со-

гласно отчету IBM 2022 г., средняя стоимость утечки данных составила 4,35 миллиона долларов, что свидетельствует о масштабах проблемы. Такие инциденты не только наносят материальный ущерб, но и создают чувство незащищенности среди граждан, усиливая их тревожность и недоверие к цифровым технологиям. Тем не менее, «местные власти нуждаются в информации, которая исследует местные контексты и проблемы преступности и насилия, что наблюдательные органы по преступности и социальным проблемам стремятся предоставить» (Sagat, Shaw, 2010. 42 с.). Это подчеркивает важность комплексного подхода к изучению киберпреступности и ее влияния на общество, учитывающего не только экономические, но и социальные аспекты.

Совместные операции правоохранительных органов США и Великобритании в борьбе с киберпреступностью демонстрируют высокую эффективность и значимость международного сотрудничества. Одним из ярких примеров является операция 2020 г., проведенная Федеральным бюро расследований (ФБР) и Национальным агентством по борьбе с преступностью Великобритании (NCA), которая привела к закрытию крупнейшего нелегального интернет-рынка AlphaBay. Этот проект позволил не только ликвидировать платформу, но и задержать ключевых участников преступной сети. В 2019 г. благодаря координации между этими агентствами была разоблачена международная сеть по распространению вредоносного программного обеспечения Emotet. Эта операция предотвратила значительные финансовые потери и нанесла серьезный удар по организованной киберпреступности. Также в 2018 г. взаимодействие британских и американских служб позволило предотвратить масштабные кибератаки на финансовые учреждения в Лондоне и Нью-Йорке, что подчеркнуло важность оперативного обмена информацией и совместного планирования действий.

В ходе совместных операций правоохранительные органы США и Великобритании применяют передовые методы и технологии для выявления и пресечения киберугроз. Ключевым аспектом таких операций является использование аналитических платформ, которые обрабатывают большие объемы данных, позволяя эффективно отслеживать действия киберпреступников. Например, в операции по ликвидации AlphaBay активно использовались технологии мониторинга транзакций в даркнете и методы цифровой криминалистики, что способствовало идентификации ключевых участников и их местоположения. В операции против сети Emotet применялись системы для анализа вредоносного кода, что дало возможность выявить уязвимости в инфраструктуре сети и успешно ее нейтрализовать. Эти примеры подчеркивают важность технологической оснащенности и профессиональной подготовки сотрудников правоохранительных органов для успешного противодействия киберпреступности. Ани отмечает, что «киберпреступность не отличается от традиционной преступности, при этом при глубоком анализе можно выделить явное различие, заключающееся в вовлечении виртуальной среды в случаи киберпреступлений» (Ани, [б. г.], 5 с.).

Успешные совместные операции правоохранительных органов США и Великобритании иллюстрируют потенциал международного сотрудничества в борьбе с киберпреступностью. Они показывают, что объединение усилий, обмен опытом

и технологиями позволяют достигать значительных результатов в противодействии сложным киберугрозам. Такие операции способствуют укреплению доверия между странами и создают основу для дальнейшего развития сотрудничества. Кроме того, успешные кейсы, такие как ликвидация AlphaBay или разоблачение сети Emotet, служат примерами для других государств, демонстрируя, как можно эффективно организовать взаимодействие в условиях глобальной цифровой экономики. Это подчеркивает необходимость продолжения работы в данном направлении и совершенствования механизмов международного сотрудничества.

Недостаток финансовых и технических ресурсов представляет собой значительное препятствие в борьбе с киберпреступностью. Современные киберугрозы требуют применения передовых технологий и высококвалифицированных специалистов, и правоохранительные органы часто сталкиваются с ограничениями в этих областях. Согласно отчету Europol за 2020 г., нехватка ресурсов затрудняет осуществление эффективных операций, особенно в мегаполисах с высоким уровнем киберпреступности. Это обуславливает необходимость крупных инвестиций в технологические разработки и повышение квалификации кадров, а также необходимость составления совместных программ преодоления нынешних ограничений. Так, Finklea и Theohary отмечают, что «в течение более трех десятилетий Конгресс беспокоился о киберпреступности и связанных с ней угрозах», это указывает на приоритетность комплексного подхода к обеспечению кибербезопасности и выделению ресурсов на поставленную задачу. Координация правоохранительных органов США и Великобритании также не без трудностей, особенно в вопросах, связанных с обменом информацией. Различия в стандартах процессуальных документов обмена часто приводят к задержкам и затруднениям. Например, совместная операция между ФБР и NSA 2018 г. была затруднена проблемами в координации из-за различия в процедурах обмена данными. Подобные проблемы показывают, что необходимо унифицировать протоколы и стандарты, которые обеспечивают взаимодействие между странами, что повысит эффективность операций.

Современная киберпреступность ставит все более сложными и масштабными задачи, что требует своевременной адаптации своих действий от правоохранительных органов. Исходя из отчета Cybersecurity Ventures, ущерб, наносимый киберпреступлениями, может достигать 10,5 триллионов долларов ежегодно с 2025 г., а это довольно значимая проблема. В условиях глобализации и взаимосвязи информационных систем преступники применяют различные достижения технологий в сфере искусственного интеллекта и блокчейна, для осуществления атак, что значительно затрудняет противодействие им. На основе анализа современных вызовов следует сказать, что подходы к борьбе с киберугрозами необходимо пересматривать и совершенствовать, особенно в таких местах как мегаполисы, ведь там огромное скопление информационной инфраструктуры.

Для повышения эффективности противодействия киберпреступности необходимо совершенствовать стратегии сотрудничества и подстраивать их под ситуацию. Если говорить об успешном взаимодействии, можно привести такой пример как совместная операция 2021 г. по ликвидации группы киберпреступников, которые использовали программы-вымогатели. Под адаптацию стратегий отнести

более быстрый и тесный обмен информацией и использование только передовых технологий для анализа данных, а также проведение совместных тренировок. Согласно Элегбе, «технология является дикой и столь же продвинутой, как и государство. Следовательно, власти или законодатели занимаются пересмотром или изменением старых и новых административных правонарушений» (2024. 2 с.). Такие меры позволят повысить эффективность действий правоохранительных органов, особенно в мегаполисах, где масштабы и последствия кибератак могут понести больший вред, чем в маленьких городах.

В заключение следует отметить, что проведенный анализ различных аспектов взаимодействия стран демонстрируют значимость подобного сотрудничества. Также подтверждается мысль о том, что эффективное сотрудничество стран – один из ключевых факторов противодействия преступлениям в сфере кибербезопасности, а изучение путей обмена информацией позволит повысить эффективность взаимодействия стран.

Список литературы

1. Finklea K. M., Theohary K. A. Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement / Congressional Research Service. – [б. м.]: [б. и.], 2012. — [б. с.].
2. Sagat V., Shaw M. International Report on Crime Prevention and Community Safety: Trends and Perspectives / Valérie Sagant, Margaret Shaw. – М.: International Centre for the Prevention of Crime, 2010. – 150 с.
3. Świątkowska J. Tackling cybercrime to unleash developing countries' digital potential // Pathways for Prosperity Commission Background Paper Series; no. 33. – Оксфорд, Великобритания, 2020. – [Электронный ресурс]. – URL: www.pathwayscommission.bsg.ox.ac.uk.
4. https://ciaotest.cc.columbia.edu/wps/ewi/0021724/f_0021724_17971.pdf
5. Каун П. Н. Анализ подготовки армии США к операциям в мегагородах: исследовательский проект / П. Н. Каун. – [б. м.]: [б. и.], 2016. – [б. с.].
6. Лаура Ани. Cyber Crime and National Security: The Role of the Penal and Procedural Law // Law and Security in Nigeria. – [б. г.]. – [б. м.]. – [б. и.].
7. Элегбе И. Ц. Законодательство о киберпреступности: сравнительный анализ правовых рамок, политических ответов и рекомендаций // International Journal of Education and Social Science Research. – 2024. – Т. 7, Вып. 2. – С. 199–207. [Электронный ресурс]. – URL: <https://ijessr.com>.

Воробьева Д. С.¹,
курсант 943 взвода 1 курса
Московского университета МВД России имени В.Я.Кикотя

Научный руководитель:
Куликов В. Н.,
преподаватель кафедры иностранных языков
Московского университета МВД России
имени В.Я.Кикотя

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ

Основные понятия, которые относятся к теме безопасного поведения в сети интернет и описывают виды киберпреступлений:

Киберпреступления – противоправные действия, совершаемые с использованием компьютерных технологий, включая нарушения информационной безопасности, кражи через цифровые средства, шантаж, вымогательство, а также создание и распространение запрещенных материалов.

Фишинг – вид мошенничества, направленный на получение конфиденциальной информации (данных для доступа к электронной почте, социальным сетям, интернет-банкингу) путем обмана.

Вишинг (англ. vishing – voice + phishing) – разновидность фишинга, осуществляемая через телефонные звонки, где злоумышленники, применяя методы социальной инженерии и представляясь сотрудниками банков или специалистами, вынуждают жертву раскрыть личные или банковские данные либо совершить действия с финансами.

Информационная безопасность – состояние защищенности интересов личности, общества и государства от угроз в информационной среде.

Кибератака – целенаправленное воздействие на информационные системы или сети с целью нарушения их работы или создания угроз для хранимой информации.

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Киберинцидент – событие, угрожающее конфиденциальности, целостности или доступности информации, а также нарушающее политики безопасности.

Кибертерроризм – атаки на информационные системы, создающие угрозу жизни и здоровью людей, способные нарушить работу ключевых объектов для воздействия на органы власти, устрашения населения или дестабилизации порядка.

Конфиденциальность информации – требование предотвращать несанкционированное распространение данных без согласия их владельца.

¹ © Воробьева Д. С., 2025.

Персональные данные – сведения о физическом лице, позволяющие его идентифицировать, включая информацию, подлежащую регистрации в соответствии с законом.

Пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею.

Пользователь информационной системы и (или) информационной сети – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими.

Предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц.

Преступления в информационной сфере – предусмотренные Уголовным кодексом Российской Федерации преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети.

Распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц.

Смишинг – вид мошенничества (англ. smishing – SMS + phishing), целью которого является переход по ссылке из SMS и/или загрузки вредоносного программного обеспечения.

Цифровая гигиена – совокупность правил, обеспечивающих защиту пользователя в интернете через осознанное поведение и знания о безопасности [1].

В последние годы наблюдается устойчивый рост киберпреступлений. Согласно данным аналитических исследований, в первой половине 2024 года число инцидентов увеличилось на 7 % по сравнению с предыдущим годом. Основные тенденции включают:

Рост утечек данных, например в 2024 году 72 % успешных атак на частных лиц и 54 % на организации привели к утечке конфиденциальной информации. Это связано с увеличением использования троянов удаленного управления (RAT), таких как Quasar RAT и SugarGh0st.

Также снижение доли шифровальщиков: если в 2023 году шифровальщики составляли 73 % атак в некоторых отраслях (например, транспорт), то в 2024 году их доля сократилась до 44 % в атаках на организации, уступив место шпионскому ПО (47 %).

Выросло количество фишинговых атак, так во второй половине 2024 года доля фишинговых сайтов в атаках на частных лиц выросла на 11%, достигнув 73 %.

Влияет также геополитический фактор – в странах : России (73 % атак в регионе), Казахстане (8 %) и Беларуси (7 %), кибератаки в 2024 году усилились на фоне напряженной геополитической обстановки.

Экономический ущерб растет. В России прямой ущерб от киберпреступлений в 2024 году превысил 200 млрд рублей, что на 36 % больше, чем в 2023 году. Общий ущерб оценивается в 250–300 млрд рублей [2].

Обучение сотрудников станет основной целью, так как 50 % атак на организации и 92 % на частных лиц в 2024 году использовали социальную инженерию.

Экономический ущерб в России может снизиться благодаря внедрению национальной антифрод-платформы [2].

Эти правила должны соблюдать все граждане, чтобы не попасться в руки мошенников [3].

Правило № 1. Храните пароли и коды в тайне.

ПИН-код карты – это конфиденциальная информация, которую нельзя никому раскрывать. Он служит секретным ключом для доступа к вашим средствам, поэтому его следует запомнить, а не записывать на бумаге или другом носителе и носить с собой. Вводя ПИН-код в банкомате или магазине, всегда прикрывайте клавиатуру рукой.

На обратной стороне карты указан CVC/CVV-код – три цифры, необходимые для онлайн-покупок. Чтобы злоумышленники не смогли воспользоваться вашими деньгами, никогда не сообщайте и не показывайте этот код никому.

Сотрудники банка никогда не запрашивают ПИН-код, CVC/CVV-код или коды из SMS, отправленных банком. Такие данные интересуют только мошенников. Они могут выдавать себя за кого угодно — от банковских работников до родственников, друзей или даже людей, попавших в беду, лишь бы выдать секретные сведения.

Иногда мошенники притворяются знакомыми, желающими якобы перевести вам деньги на карту, и просят сообщить номер карты, срок действия и CVC/CVV-код. Это обман: для перевода достаточно только номера карты, другие данные – срок действия, имя владельца или код – не нужны.

Правило № 2. Хранение и использование банковской карты.

Обращайте внимание на условия хранения и эксплуатации карты. Избегайте механических повреждений, воздействия высоких или низких температур, электромагнитных полей и влаги. Не размещайте карту рядом с мобильными телефонами, бытовой или офисной техникой.

Пользуйтесь только банкоматами, установленными в государственных учреждениях, отделениях банков, гостиницах или крупных торговых центрах. Использование изолированного банкомата на темной улице может привести к риску стать жертвой мошенничества или даже нападения.

Если банкомат задержал карту, не выдал деньги или выдал сумму, не соответствующую запросу, обратитесь по номеру телефона, указанному на наклейке банкомата. Запишите данные устройства, дату, точное время операции и запрошенную сумму, а затем сообщите об этом родителям. Именно поэтому предпочтительнее пользоваться банкоматами в банковских отделениях – там можно сразу получить помощь от сотрудников.

Если вы забыли ПИН-код, не пытайтесь вводить его трижды. После трех неверных попыток банкомат заблокирует карту.

Не удаляйте защитный слой с обратной стороны карты, иначе ее не примут к оплате [3].

Правило № 3. Активируйте SMS-уведомления по карте.

Это позволит мгновенно получать от банка сообщения о любых операциях с картой, например о покупках. Внимательно проверяйте эти уведомления. Если

вы получите сообщение о транзакции, которую не совершали, вероятно, картой воспользовались мошенники.

Немедленно сообщите родителям о подозрительном уведомлении. Они свяжутся с банком и попросят заблокировать карту.

Установите дневной лимит на снятие наличных – это ограничит сумму, которую мошенники смогут снять, если получат доступ к карте.

Правило № 4. Будьте внимательны при взаимодействии с третьими лицами.

Никогда не передавайте свою карту посторонним. Держите ее под контролем и не демонстрируйте ее данные. Злоумышленники могут скопировать реквизиты карты и использовать их, особенно для онлайн-покупок.

Правило № 5. Совершайте покупки только с личных устройств.

Для оплаты покупок, входа на сайт банка или в приложение используйте только собственный компьютер, планшет или телефон. Защитите все свои устройства паролями.

Если вы потеряли телефон или планшет, на котором установлено банковское приложение или приходят уведомления с паролями, срочно сообщите родителям. Они должны связаться с банком, чтобы отключить услуги, привязанные к номеру телефона, и заблокировать доступ к счету с утерянного устройства. Обновите логин и пароль для интернет-банка. После восстановления номера у оператора связи можно будет вновь подключить SMS-уведомления.

Правило № 6. Избегайте переходов по подозрительным ссылкам.

Не открывайте ссылки из писем или сообщений от незнакомцев – это может быть вредоносное ПО, крадущее личные данные.

Даже если ссылку прислал знакомый, не спешите ее открывать. Мошенники могли взломать аккаунт и отправить сообщение от его имени. За такими ссылками часто скрываются трояны, которые устанавливаются на устройство, похищают данные и даже переводят деньги злоумышленникам.

Правило № 7. Не торопитесь и проверяйте информацию.

Мошенники рассчитывают на вашу доверчивость и спешку, чтобы вы не успели проверить их слова. В финансовых вопросах торопиться нельзя. Не передавайте секретные данные карты и не переводите деньги, пока не убедитесь в ситуации. Посоветуйтесь с родителями. Главное – сохраняйте спокойствие и осмотрительность[4].

Одной из мер является внедрение систем раннего выявления угроз, например SIEM (Security Information and Event Management), и автоматизированных платформ реагирования.

Также в обязательном порядке нужно повышать киберграмотность граждан для минимизации случаев мошенничества, взломов и т. д.

Принимать регуляторные меры, то есть ужесточить законодательство, включая уголовную ответственность за использование дипфейков и обязательное уведомление об утечках данных.

Обмениваться разведданными о киберугрозах между странами для борьбы с транснациональными группировками.

Таким образом, можно сделать вывод, что киберпреступность в 2024–2025 гг. демонстрирует динамичный рост, обусловленный развитием технологий, геополитическими факторами и неосведомленностью граждан в сфере информационных технологий. Основные угрозы включают фишинг и вредоносное ПО, а ущерб достигает сотен миллиардов рублей ежегодно. Прогнозы на 2025 год указывают на необходимость усиления мер противодействия киберпреступлениям через обучение граждан новейшим технологиям, проведение профилактики киберпреступлений и ужесточение законодательства в сфере киберпреступности. Только комплексный подход позволит минимизировать риски и обеспечить кибербезопасность в условиях цифровизации [4].

Список литературы

1. Официальный интернет-сайт МВД России [Электронный ресурс]. URL: <https://мвд.рф/> (дата обращения: 21.03.2025).
2. Проблемы противодействия киберпреступности [Электронный ресурс]. URL: https://academy-skrf.ru/about_the_university/news/ (дата обращения: 21.03.2025).
3. Способы противодействия киберпреступности [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/sposoby-protivodeystviya-kiberprestupnosti/viewer> (дата обращения: 21.03.2025).
4. Профилактика и противодействие киберпреступлений [Электронный ресурс]. URL: <https://ds-raduga-yugorsk-r86.gosweb.gosuslugi.ru/> (дата обращения: 21.03.2025).

Горкина У. Р.¹,

курсант международно-правового факультета

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Воротникова И. Г.,

доцент кафедры иностранных языков

Московского университета

МВД России имени В.Я. Кикотя,

кандидат филологических наук, доцент

ПРАВОВЫЕ ПРОБЛЕМЫ И МЕРЫ РЕАГИРОВАНИЯ НА КИБЕРПРЕСТУПНОСТЬ В КАНАДЕ

Киберпреступность растет по всему миру, включая и Канаду. Преступления такого рода затрагивают как физических лиц, так и предприятия по всей стране. Несмотря на то, что киберпреступность во всем мире имеет общие черты, в каждой стране она уникальна.

Канада занимает довольно высокие позиции с точки зрения кибербезопасности. В сравнении, проведенном компанией Comparitech, в котором учитывались 75 стран и более десятка факторов, Канада заняла 13-е место. В число факторов входили степень готовности страны к кибератакам и частота кибератак [1]. В исследовании, опубликованном IT World Canada, Канада заняла пятое место после Соединенных Штатов. Однако в это исследование по кибербезопасности были включены только двадцать стран [1]. Недавний отчет Статистического управления Канады показал, что в период с января по июнь 2024 года в полицию Канады поступило более 41 000 сообщений о киберпреступлениях. Большинство из этих нарушений были мошенничеством, что составило 56% от общего числа нарушений [1].

По данным Канадского центра по борьбе с мошенничеством, в 2021 г. канадцы потеряли из-за мошенничества около 230 миллионов долларов. Более 100 миллионов долларов было связано с онлайн-мошенничеством. Наиболее распространенным онлайн-мошенничеством было инвестиционное мошенничество, стоимость которого оценивалась в 70 миллионов долларов. Мошенничество с онлайн-инвестициями все чаще связано с криптовалютами [1].

Согласно опросу пользователей Интернета в Канаде, 57,3 % канадцев сталкивались, по крайней мере, с одним инцидентом, связанным с безопасностью в Интернете. Наиболее распространенным типом сообщений были фишинговые электронные письма и текстовые сообщения, причем 48 % респондентов сообщили, что получали подозрительные электронные письма. Подсчитано, что 91 % всех кибератак начинаются с мошеннических электронных писем. 18,7 % респондентов были перенаправлены на мошеннические веб-сайты, а 11,4 % заявили, что столкнулись с вирусами и вредоносными программами. У 5,7 % канадцев были

¹ © Горкина У. Р., 2025.

взломаны учетные записи, а 4,5 % стали жертвами киберпреступлений. В настоящее время случаи кражи личных данных в Канаде по-прежнему редки, ведь только 2 % респондентов стали жертвами кражи личных данных [1].

Канада часто сталкивается с растущей угрозой кибершпионажа и кампаний по дезинформации. Однако канадским правоохранительным органам, включая Королевскую канадскую конную полицию (далее – КККП), с трудом удается справляться с растущей прогрессивностью и частотой подобных нападения.

Национальный координационный центр КККП по борьбе с киберпреступностью (NC3) и другие подразделения работают над выявлением, пресечением и расследованием данной деятельности. Несмотря на эти усилия, быстрое развитие киберугроз опережает настоящие возможности и ресурсы канадских ведомств. Проблемы включают нехватку специализированного персонала, недостаточность финансирования и необходимость улучшения координации между федеральным и муниципальным уровнями [3].

Одной из основных проблем в борьбе с киберпреступностью является нехватка квалифицированных специалистов по кибербезопасности. Для этой области требуются люди, обладающие специальными знаниями в различных областях, таких как цифровая криминалистика, реагирование на инциденты, связанные с кибератаками, анализ угроз. Спрос на эти навыки сильно превышает предложение, что приводит к значительным пробелам в рабочей силе. Эта нехватка препятствует возможности агентств быстро и эффективно реагировать на кибератаки. Чтобы решить эту проблему, правительство Канады финансирует образовательные программы, направленные на формирование кадров, способных решать сложные киберзадачи. Такое финансирование включает в себя стипендии для студентов, изучающих кибербезопасность, партнерские отношения с учебными заведениями и специализированные учебные курсы для сотрудников правоохранительных органов. Несмотря на эти усилия, стремительные темпы развития киберугроз требуют постоянного обучения, ведь главная задача перед канадскими правоохранительными органами – опережать киберпреступников [3].

Финансирование в данную сферу также необходимо для развития и поддержания надежной инфраструктуры кибербезопасности. Однако многие канадские агентства сталкиваются с бюджетными барьерами, которые ограничивают их возможность инвестировать в передовые технологии и инструменты, необходимые для эффективной киберзащиты. Это включает ресурсы для обнаружения угроз, систем мониторинга и реагирования на инциденты. Недостаточное финансирование также влияет на возможность проводить комплексные исследования и разработки, чтобы опережать возникающие угрозы [3]. Увеличение финансирования могло бы способствовать закупке современных средств кибербезопасности, расширению кибернетических подразделений и улучшению возможностей по анализу угроз. Оно также способствовало бы более тесному сотрудничеству с партнерами из частного сектора, которые обладают передовыми технологиями и опытом. Более того, увеличение финансовых ресурсов, выделяемых на кибербезопасность, могло бы привлечь самых талантливых специалистов в этой области, решив проблему нехватки персонала.

Кроме того, эффективная киберзащита требует четкой координации между федеральными и муниципальными органами власти, а также организациями частного сектора. Однако разобщенность операций часто препятствуют обмену информацией. В разных частях страны могут быть разные протоколы, возможности и приоритеты, что затрудняет единое реагирование на киберугрозы. Чтобы смягчить эти проблемы, Канада работает над созданием более надежных каналов связи и стандартизированных процедур отчетности о кибератаках и реагирования на них. Создание централизованных органов, таких как NC3, направлено на оптимизацию усилий по координации и служит центром для обмена ресурсами. Укрепление партнерских отношений между государственным и частным секторами также имеет юольшое значение, так как предприятия часто располагают очень важными данными и инфраструктурой, которые требуют защиты и сотрудничества [3].

Однако киберпреступники постоянно совершенствуют свои методы, используя сложные инструменты и стратегии для взлома систем защиты. Скорость, с которой развиваются эти технологии, часто опережает существующие защитные меры, из-за чего канадские агентства с трудом успевают за ними. Методы киберпреступников постоянно расширяются, и противостоять им становится намного труднее. Инвестиции от иностранных государств в разработки по кибербезопасности необходимы для того, чтобы идти в ногу с этими методами. Оставаясь в курсе последних киберугроз и разрабатывая инновационные механизмы защиты, Канада сможет улучшить защиту своей цифровой среды. Сотрудничество с международными союзниками и участие в глобальных форумах по кибербезопасности также играют важнейшую роль в обмене знаниями и опытом в борьбе с возникающими угрозами.

Кроме того, канадские власти разработали комплексный подход к решению проблем, связанных с киберпреступностью. Эта стратегия включает в себя скоординированные усилия государственных учреждений, правоохранительных органов и кампаний по просвещению общественности, каждая из которых направлена на защиту граждан, предприятий и критической информационной инфраструктуры. Национальная стратегия кибербезопасности подчеркивает участие Канады в защите своих граждан от киберугроз. Эта инициатива направлена на создание безопасной и устойчивой цифровой экосистемы посредством определенных мер [4].

Канадский центр кибербезопасности выполняет функции основного центра по кибербезопасности. Он предоставляет техническую поддержку и консультации частным лицам, предприятиям и государственным учреждениям, предлагает практические рекомендации организациям и разрабатывает ресурсы для повышения общей киберустойчивости. В настоящее время особо важен обмен опытом и инструментами для повышения осведомленности о кибербезопасности и готовности к ней. В совокупности эти усилия обеспечивают защиту от киберугроз [4].

Законодательство Канады также претерпевает изменения. Были приняты законы, направленные на борьбу с растущей проблемой киберпреступности. Уголовный кодекс Канады направлен на предотвращение несанкционированного до-

ступа к компьютерам, распространения вредоносных программ и перехвата данных, предоставляя правоохрательным органам необходимые инструменты для эффективного расследования киберпреступлений и судебного преследования киберпреступников [2].

Достижение баланса между общественной безопасностью и неприкосновенностью частной жизни остается главной задачей и при разработке и применении законов о киберпреступности. Несмотря на существующую правовую базу, расследование случаев киберпреступлений и судебное преследование киберпреступников довольно сложны. Безграничность сети Интернета часто означает, что преступники могут действовать из разных уголков мира, что делает практически невозможным их распознать. Более того, динамичная и быстро меняющаяся тактика, используемая киберпреступниками, требует постоянного совершенствования со стороны правоохрательных органов. Идти в ногу с технологическим прогрессом и разнообразием киберугроз остается постоянной задачей канадских властей [2].

Еще одной важной задачей правоохрательных органов является информирование общественности. Правительственные учреждения и некоммерческие организации Канады активно участвуют в инициативах, направленных на ознакомление частных лиц и компаний с передовым опытом в области кибербезопасности, повышение осведомленности о киберугрозах, поощрение ответственного поведения в Интернете и предоставление ресурсов для сообщения о киберпреступлениях [4].

Таким образом, проблема киберпреступности в Канаде требует определенных правовых решений. По мере развития технологий необходимо адаптировать правовую базу к инновациям, повышать осведомленность общественности и укреплять международное сотрудничество.

Список литературы

1. Cyber Crime Statistics in Canada. 2025. URL: <https://madeinca.ca/cyber-crime-canada-statistics/>.
2. The legal challenges and responses to cybercrime in Canada. 2023. URL: <https://theinscribermag.com/the-legal-challenges-and-responses-to-cybercrime-in-canada/>.
3. Canadian agencies struggle to combat cybercrime. 2024. URL: <https://mackenzieinstitute.com/2024/06/canadian-agencies-struggle-to-combat-cybercrime/>.
4. How Canada is Battling Cybercrime – Which Industries Are Most Vulnerable? URL: <https://canadacrimeindex.com/how-canada-is-battling-cybercrime/>.

Горшенева И. А.¹,

заведующий кафедрой иностранных языков

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, профессор,

Заслуженный работник Высшей школы РФ

Гавриленков И. С.²,

курсант 342 учебного взвода 1 курса

института подготовки сотрудников

для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ КИБЕРПРЕСТУПЛЕНИЙ: ОБЗОР ВОЗМОЖНОСТЕЙ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ

Киберпреступность становится одной из самых сложных социальных проблем информационного века. В отличие от традиционных преступлений, проявления киберпреступности могут происходить в разных юрисдикциях и географических регионах. Киберпреступность – это любое противоправное деяние, в ходе которого используется компьютер, цифровые устройства и Интернет в качестве канала совершения [1]. Данный вид противоправных действий относится к категории современных преступлений, порожденных развитием Интернета и связанных с ним технологий. Киберпреступления могут быть классифицированы как гибридные преступления в том смысле, что в отличие от традиционных уголовных правонарушений, таких как кража и грабеж, с четкой локализацией в пространстве и времени совершения, эти преступления могут иметь взаимосвязь, которую довольно трудно локализовать. Киберпреступность способна быть агрессивной, всепроникающей и вездесущей в обществе, и ее природа кажется почти бесконечной, что, в свою очередь изменяет черты социально-политических и поведенческих характеристик обычных преступлений, поскольку они приводят к большим экономическим потерям в социуме [2]. Киберпреступность – это сложное и постоянно меняющееся явление, где киберпреступники становятся все более изощренными, сосредотачивая свое внимание на государственных и частных организациях, что требует от общества и правоохранительных органов дополнительных уровней защиты.

По данным Международного союза электросвязи [5], борьба с киберпреступностью является неотъемлемым компонентом стратегии кибербезопасности как критически важной информационной инфраструктуры любой страны. В частности, задачи сокращения или искоренения киберпреступности в киберпространстве должны повлечь за собой принятие соответствующих действий законодателей и других механизмов, способных обеспечивать предотвращение подобных киберпреступлений. Следует отметить, что международный союз электросвязи

¹ © Горшенева И. А., 2025.

² © Гавриленков И. С., 2025.

подчеркивает, что киберпреступность и кибербезопасность являются неразделимыми понятиями, поэтому в настоящей статье основное внимание уделяется усилиям последнего десятилетия по выявлению, пресечению и предотвращению киберпреступлений, особенно в том, что касается использования моделей машинного обучения.

Использование машинного обучения для выявления и предотвращения киберпреступлений предполагает расширение функций компьютерной системы путем ввода больших объемов данных в алгоритм, результатом которого выступает модель, используемая для выполнения интеллектуальных задач, не поддающихся традиционному программированию. В машинном обучении часто используются статистические, вероятностные и другие инструменты оптимизации, позволяющие создавать механизмы, способные извлекать уроки из шаблонов в обучающем наборе данных с целью классификации новых данных, представленных по результатам обучения. Хотя в основе машинного обучения лежат статистика и теория вероятности, она превратилась в более мощную технологию, позволяющую создавать интеллектуальные системы вывода и поддержки принятия решений с использованием прогностических моделей, что практически невозможно при обычных методах [4]. Статистические модели ограничены наборами данных, которые содержат нелинейные, взаимозависимые и условные переменные, типичные для большинства таких систем.

За прошедшие годы машинное обучение трансформировалось в оптимально фундаментальные элементы решений на основе искусственного интеллекта, используемых в настоящее время для выявления и пресечения киберпреступлений, включая такие их виды, как кибербуллинг, кибертерроризм, детская порнография, фишинг, атаки типа «отказ в обслуживании» и аналогичные угрозы юридическим и физическим лицам и обществу в целом. Обнаружение и анализ киберпреступлений стали возможны благодаря использованию аналитических данных, машинного обучения и других инновационных методик. При разработке и внедрении указанной системы использовались алгоритмы классификации, кластеризации и контроля. Исследователи выявили различные виды киберпреступлений, а также предложили рекомендации и методы их предотвращения.

После изучения сильных и слабых сторон машинного обучения был предложен подход «единого окна». Предлагаемое «единое окно» - это абстракция, представляющая собой модель стратегии борьбы с киберпреступностью, включающая в себя целый ряд разрозненных методов и механизмов сдерживания угрозы данного вида преступности. Другой стороной «единого окна» является корпоративность в том смысле, что оно обеспечивает своего рода киберплатформу, способная соединить различные экономически заинтересованные стороны, особенно предприятия и общественные организации, предоставляющие полезные услуги населению (например, судебную систему и т. д.) с помощью электронных платформ. Электронная платформа будет использовать протоколы, отличные от веб-протоколов. До внедрения машинного обучения для выявления киберпреступлений и борьбы с ними использовались независимые методы борьбы с киберпреступностью или их совокупность, такие как:

1. Законодательство о киберпреступности, например, Общие правила защиты данных в Европе, Закон о предотвращении киберпреступности 2015 года и т. д. [7]. Законодательство обеспечивает правовую базу нормативного регулирования киберпреступности и контроля за ней. Несмотря на то, что законы являются действенными инструментами, они могут не получить единого глобального признания, силы и применения соответственно. Это связано с тем, что то, что считается киберпреступлением в одной юрисдикции, может не являться преступлением в другой юрисдикции.

2. Однако из-за транснационального характера многих киберпреступлений эти международно признанные и законодательно установленные киберпреступления необходимо будет выделить в отдельный раздел «сферы киберпреступности». В указанной области характеристики известных киберпреступлений должны быть определены и зафиксированы таким образом, чтобы быть доступными, возможно, через защищенный электронный канал обмена данными и в определенной степени пригодны для принятия решений. Это означает, что предприятия и организации, работающие в общедоступных сетях, таких как Интернет, могут подключиться к указанной платформе EDI для противодействия киберпреступности. Такая платформа способна содействовать укреплению действующих национальных законов путем определения сфер гармонизации заинтересованных сторон, т.е. между одной страной или юрисдикцией и другой, тем самым продвигая концепцию обоюдной уголовной ответственности, которая была бы взаимовыгодной для участвующих сторон, а также для развития более эффективных органов управления. Платформа также укрепила бы партнерство и международное сотрудничество частного и государственного сектора [6].

3. Политика и стратегия кибербезопасности. Рассмотрим пример Нигерии. Используемая в этой стране модель «единого окна» включает в себя детали и измеримые элементы региональной или национальной стратегии кибербезопасности таким образом, чтобы они отражали критерии и основные меры реагирования, которые будут применяться индивидуально или коллективно в отношении существующих или предполагаемых киберугроз, атак и преступлений, направленных на нарушение целостности электронных транзакций, конфиденциальности, критически важных данных, инфраструктуры, защиты прав потребителей и информации. Контрольные показатели следует периодически перепроверять, соотнося их с фактическими мерами реагирования на кибератаки, задокументированные или сообщенные участвующими заинтересованными сторонами.

4. Правоохранительная деятельность: использование государственных и частных групп и агентств. К примеру, Комиссия по экономическим и финансовым преступлениям пользуется популярностью в Нигерии в борьбе с киберпреступлениями. Киберпреступность как транснациональная угроза требует наличия платформы для участия в расследованиях и возможного вмешательства из любой точки мира.

Банк угроз может быть использован в машинном обучении для создания динамичных самоадаптивных решений по борьбе с киберпреступностью. Более того, поскольку киберпреступность имеет как национальные, так и международ-

ные аспекты, единая интегрированная стратегия могла бы дать всем заинтересованным сторонам полезную информацию для разработки законодательства, политики и внедрения практических механизмов предотвращения, выявления и борьбы с этим сложным явлением в различных юрисдикциях. С этой целью самоадаптирующаяся система была бы очень полезна, поскольку она подстраивалась бы под динамику киберугроз и характер атак.

Таким образом, сторонам, заинтересованным в предотвращении киберпреступлений, необходимо сотрудничать в целях создания инфраструктуры «единого окна», которая позволила бы в максимально возможной степени отслеживать киберпреступную деятельность и предотвращать ее, устранив нехватку данных в важнейшей области исследований, сотрудничества и правоприменения.

Список литературы

1. Adil M., Khan R., Ghani M. A. N. U. Preventive techniques of phishing attacks in networks. Paper presented at the 2020 3rd International Conference on Advancements in Computational Sciences (ICACS). 2020. URL: <https://doi.org/10.1109/ICACS47775.2020.9055943>.
2. Aiyanyo I. D., Samuel H., Lim, H. A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning // Applied Sciences, 2020, No 10(17), p. 5811. URL: <https://doi.org/10.3390/app10175811>.
3. Apau R., Koranteng F. N. An overview of the digital forensic investigation infrastructure of Ghana // Forensic Science International: Synergy, 2020, No 2, pp. 299-309. URL: <https://doi.org/10.1016/j.fsisyn.2020.10.002>.
4. Chen D., Wawrzynski P. Cyber security in smart cities: A review of deep learning based applications and case studies / Sustainable Cities and Society, 2020, No 66. URL: <https://doi.org/10.1016/j.scs.2020.102655>.
5. International Telecommunication Union. Understanding cybercrime: Phenomena, challenges and legal response. 2014. URL: <https://www.itu.int/en/ITU/Cybersecurity/Pages/legislation.aspx>.
6. Nwankwo W. A Review of Critical Security Challenges in SQL-based and NoSQL Systems from 2010 to 2019 / International journal of advanced trends in computer science and engineering, 2020, No 9(2). URL: <https://doi.org/10.30534/ijatcse/2020/174922020>.
7. Nwankwo W., Njoku C. C. Adoption of Internet Voting Platform Containing Data Injection Threats with Structured LINQ // Nigerian Research Journal of Engineering and Environmental Sciences. 2019, No 4(2), pp. 724-739. URL: <http://www.rjees.com/download/?file=V04-N02-724-739.pdf>.
8. Prasad R., Rohokale V. Artificial intelligence and machine learning in cyber security // Cyber Security: The Lifeline of Information and Communication Technology, Springer, 2020, pp. 231-247. URL: https://doi.org/10.1007/978-3-030-31703-4_16.

Грунина А. М.¹,
*курсант международно-правового факультета
Московского университета МВД России
имени В. Я. Кикотя*

Научный руководитель:
Хмирова Е. А.,
*старший преподаватель кафедры иностранных языков
Московского университета МВД России имени В. Я. Кикотя*

ПРОБЛЕМА БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В СЕРБИИ: ОСОБЕННОСТИ РЕГУЛИРОВАНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современная Сербия, как и большинство стран мира, сталкивается с растущей угрозой киберпреступности, которая становится серьезным вызовом для национальной безопасности и экономической стабильности. В последние годы страна предпринимает активные шаги по совершенствованию системы кибербезопасности, однако процесс этот сталкивается с рядом системных проблем, требующих комплексного решения.

Согласно данным сербского Министерства внутренних дел, в 2023 г. было зарегистрировано более 5,6 тыс. киберпреступлений, что на треть превышает показатели предыдущего года. Наиболее распространенными видами преступлений стали фишинг (около 40 % случаев), финансовое мошенничество (25 %), атаки с использованием вредоносного ПО (15 %) и утечки персональных данных (10 %).

Современная правовая система Сербии в сфере кибербезопасности находится в процессе активного формирования, ориентируясь на лучшие европейские практики. Основу этого процесса составило принятие в 2021 г. Закона «Об информационной безопасности», который стал концептуальной основой для защиты критической инфраструктуры республики. Этот законодательный акт ввел важные понятия «операторов важнейших услуг» и «цифровых сервис-провайдеров», установив для них особые требования по управлению киберрисками, а также обязательства по уведомлению о инцидентах (в течение 72 часов) и необходимости разработки планов обеспечения непрерывности бизнеса. Параллельно с вышеуказанным актом в 2018 г. был принят Закон «О защите персональных данных», он практически полностью воспроизвел положения европейского GDPR (General Data Protection Regulation), включая принципы обработки данных, права субъектов данных и требования к международной передаче информации. Уголовное законодательство Сербии также было дополнено специальными нормами, предусматривающими наказание за различные виды киберпреступлений – от несанкционированного доступа (до 3 лет лишения свободы) до компьютерного

¹ © Грунина А. М., 2025.

саботажа (до 5 лет). Однако при всех этих достижениях сербское законодательство содержит существенные пробелы, наиболее заметным из которых является отсутствие комплексного регулирования операций с криптовалютами.

В отличие от стран ЕС, где уже действуют четкие правила в соответствии с Регламентом MiCA (Markets in Crypto-Assets), в Сербии до сих пор отсутствует даже базовое определение «виртуальных активов» в законодательстве. Это создает значительные проблемы для правоохранительных органов, поскольку криптовалюты активно используются преступными группировками для отмывания денег, финансирования терроризма и получения выплат при ransomware-атаках. При этом стоит отметить, что Национальный банк Сербии еще в 2020 г. выпустил предупреждение о рисках, связанных с криптовалютами, а в 2022 г. Министерство финансов представило концепцию регулирования этого сектора, однако соответствующий законопроект до сих пор не внесен в парламент. Еще одной значимой проблемой является недостаточная имплементация международных стандартов в области киберпреступности. Несмотря на подписание в 2018 г. Будапештской конвенции о киберпреступности, Сербия до сих пор не завершила процесс ее ратификации. Это создает сложности в международном сотрудничестве, особенно в вопросах экстрадиции киберпреступников и быстрого обмена информацией между правоохранительными органами.

Особого внимания заслуживает и вопрос регулирования искусственного интеллекта – в то время как ЕС уже принял Закон об ИИ (AI Act), сербское законодательство пока не содержит даже базовых норм, регулирующих эту быстро развивающуюся сферу. Перспективы развития законодательства в этой области связаны с необходимостью скорейшего принятия трех ключевых документов: Закона о цифровых активах, поправок к Уголовному кодексу (ужесточающих наказание за киберпреступления) и закона о ратификации Будапештской конвенции. Только комплексный подход, сочетающий законодательные изменения, организационные меры и международное сотрудничество, позволит Сербии создать эффективную систему противодействия современным киберугрозам. Санкции за нарушения в области защиты данных остаются недостаточно строгими – максимальный штраф составляет около 17 тысяч евро, что несопоставимо с европейскими нормами.

Также серьезной проблемой является техническое отставание. Многие государственные учреждения продолжают использовать устаревшее программное обеспечение, включая операционные системы, не получающие обновлений безопасности, ввиду чего возникает уязвимость государственного сектора Сербии.

Согласно данным аудита 2023 г., около 60 % сербских государственных учреждений продолжают эксплуатировать операционную систему Windows 7, несмотря на официальное прекращение ее поддержки корпорацией Microsoft в январе 2020 г. Эта ситуация создает серьезные риски для национальной кибербезопасности. Например, ключевыми проблемами безопасности являются, во-первых, отсутствие обновлений безопасности, ведь с момента прекращения поддержки Windows 7 не получает критически важных аспектов и усовершенствованных механизмов безопасности. Это означает, что все новые уязвимости, об-

наруженные в системе, остаются незакрытыми, предоставляя киберпреступникам постоянно расширяющийся арсенал для атак. Во-вторых, несовместимость с современными средствами защиты, многие современные решения кибербезопасности (антивирусные программы, системы обнаружения вторжений) постепенно теряют совместимость с устаревшей ОС, оставляя компьютеры без эффективной защиты. Последствия для национальной безопасности, которые вытекают из проблем старой операционной системы, следующие: угроза критической инфраструктуре, т. к. многие компьютеры с Windows 7 подключены к внутренним сетям госучреждений, создавая «точки входа» для потенциальных атак на более важные системы. Риск утечки конфиденциальных данных, а именно, устаревшая ОС не соответствует современным стандартам шифрования и защиты данных, что особенно критично для органов, работающих с персональными данными граждан. Таким образом, сохранение Windows 7 в государственном секторе Сербии представляет собой "бомбу замедленного действия" для национальной кибербезопасности. Решение этой проблемы требует не просто технического обновления, но и изменения подхода к ИТ-безопасности на институциональном уровне. Инвестиции в модернизацию сегодня помогут избежать значительно больших потерь от потенциальных кибератак в будущем.

Проблема «утечки мозгов» в сфере кибербезопасности приобрела для Сербии характер национального кризиса. Согласно данным Министерства образования за 2023 г., около 65 % выпускников ИТ-специальностей с углубленной подготовкой в области информационной безопасности покидают страну в течение первых трех лет после окончания вуза. Основными направлениями миграции становятся Германия (42 % уезжающих специалистов), Австрия (23 %) и страны Бенилюкса (18 %). При этом средняя зарплата кибербезопасника в Сербии составляет около 1,100 евро в месяц, что в 3–4 раза ниже, чем в странах ЕС для аналогичных позиций.

Особенно остро ощущается дефицит специалистов по расследованию киберинцидентов (SOC-аналитиков, криминалистов цифровых доказательств) и экспертов по защите критической инфраструктуры. Национальный CERT Сербии укомплектован лишь на 60 % от штатной численности, а в региональных отделениях ситуация еще хуже – вакансии остаются открытыми по 6–8 месяцев. Парадоксально, но именно успехи в образовательной сфере усугубляют эту проблему. Сербские технические вузы (особенно Белградский университет и Университет Нови-Сада) готовят специалистов высокого класса по программам, аккредитованным международными организациями типа (ISC) и EC-Council. Однако отсутствие карьерных перспектив и слабая материально-техническая база на рабочих местах толкают этих специалистов к эмиграции. Попытки удержать кадры через программы типа «Киберстажировки в госсекторе» (2022 г.) пока не дают значимых результатов – из 150 участников программы лишь 17 % остались работать в государственных структурах по ее окончании. Международное сотрудничество Сербии в сфере кибербезопасности развивается крайне неравномерно. Несмотря на подписание Будапештской конвенции еще в 2018 г., процесс ратификации за-

стопорился из-за необходимости внесения изменений в 12 законодательных актов. Это ограничивает участие сербских правоохранительных органов в таких ключевых механизмах, как:

1. 24/7 Network – система оперативного взаимодействия национальных
2. CERT - Совместные расследования с Europol
3. Программы обмена цифровыми доказательствами

Участие в инициативах ЕС (EU4Digital, CEPOL) носит во многом формальный характер. Из запланированных на 2021–2023 гг. 27 совместных проектов полностью реализовано лишь 9, причем в основном в области образовательных программ. Доступ к ключевым базам данных и системам раннего предупреждения (например, EISAS) остается ограниченным. Сербия не включена в систему автоматического обмена информацией о киберугрозах между странами-членами ЕС.

Проведенный анализ позволяет констатировать, что Сербия находится на сложном этапе формирования собственной системы кибербезопасности, сталкиваясь с комплексом взаимосвязанных вызовов. С одной стороны, страна демонстрирует значительный прогресс в законодательной сфере, о чем свидетельствует принятие ключевых нормативных актов. Однако на практике система сталкивается с серьезными системными проблемами. Наиболее острой остается кадровая ситуация – ежегодная эмиграция около 200 квалифицированных специалистов в области кибербезопасности подрывает способность государства эффективно противостоять угрозам. Особую озабоченность вызывает отсутствие комплексного регулирования операций с криптовалютами, которые активно используются преступными группировками. В отличие от стран ЕС, где уже действуют четкие правила в соответствии с Регламентом MiCA, в Сербии до сих пор отсутствует даже базовое определение «виртуальных активов» в законодательстве.

Список литературы

1. National Cybersecurity Center of Serbia. Cyber Threats Report 2022-2023 / Ed. by M. Petrović. Belgrade : NCCS, 2023. 112 p.
2. Ministry of Information Society and Administration of the Republic of Serbia. (2021). Law on Information Security. Official Gazette of RS, No. 54/2021. Belgrade: Government of Serbia.
3. National Assembly of the Republic of Serbia. (2018). Law on Personal Data Protection. Official Gazette of RS, No. 87/2018. Belgrade: Serbian Government Printing House.
4. Council of Europe. (2022). Budapest Convention on Cybercrime: Implementation Report - Serbia. Strasbourg: Council of Europe Publishing. 45 p.
5. Petrović, N., & Janković, S. (2023). Cybersecurity Legislation in Western Balkans: Case Study of Serbia. Belgrade: Institute of Security Studies. 156 p.
6. Jovanović D., Stojanović M. Analysis of IT Infrastructure in Serbian Public Sector // Belgrade University Journal. Series Organizational Sciences. 2023. Vol. 15, No 2. P. 45-67.

7. Ministry of Information Society and Administration of the Republic of Serbia. The annual report on the state of information security for 2023. – Belgrade, 2023. – 47 p.
8. Microsoft Corporation. The State of Legacy Systems in CSEE Region: technical report [Electronic resource]. – Redmond, 2022. – 34 p. – URL: <https://www.microsoft.com/security/reports/legacy-systems-csee> (date of access: 20.05.2024). – Text: electronic.
9. Ministry of Education, Science and Technological Development of Serbia. (2023). Annual Report on IT Workforce Migration 2023. Belgrade: Government Publishing House. – 45 p.
10. Petrović, M., & Jovanović, D. (2023). "Brain Drain in Cybersecurity: Case Study of Serbia" // Journal of Balkan Security Studies. Vol. 8. No 1. P. 23–41.

Кольяк А. П.¹,
курсант международно-правового факультета
Московского университета МВД России
имени В. Я. Кикотя

Научный руководитель:
Хмирова Е. А.,
старший преподаватель кафедры иностранных языков
Московского университета МВД России имени В. Я. Кикотя

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШЕННЫМ В ДАРКНЕТ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ В США И РОССИИ

Современное информационное общество, переживающее бурный рост технологий и всеобщую цифровизацию, столкнулось с беспрецедентными вызовами и угрозами, многие из которых напрямую связаны с анонимностью и доступностью глобальной сети Интернет. Одной из наиболее серьезных проблем, представляющих опасность для государственной безопасности и благополучия граждан, является даркнет – скрытая, завуалированная часть интернета, недоступная для обычных пользователей и стандартных поисковых систем. Это не просто «темный угол» интернета, а целая экосистема, функционирующая по своим правилам и представляющая собой серьезную угрозу как для отдельных граждан, так и для целых государств.

Даркнет – это, по сути, сеть поверх сети, построенная по принципу многоуровневой маршрутизации данных через распределенные серверы, расположенные по всему миру. Доступ к нему осуществляется с помощью специального программного обеспечения, такого как Тор, которое обеспечивает анонимность пользователей путем шифрования трафика и его перенаправления через множество промежуточных узлов. Это делает отслеживание активности пользователей в даркнете чрезвычайно сложной задачей для правоохранительных органов. В этой скрытой сети процветает преступная деятельность всех мастей, масштабы которой постоянно растут. Здесь можно найти все, что запрещено в обычном интернете: от продажи наркотиков и оружия до торговли персональными данными, заказов на киберпреступления, проведения хакерских атак и даже организации террористической деятельности. Анонимность, которую обеспечивает даркнет, создает благоприятную среду для преступников, позволяя им действовать безнаказанно, обходя традиционные методы расследования. Они общаются через зашифрованные форумы, используют криптовалюты для финансовых операций, что существенно затрудняет их идентификацию и привлечение к ответственности.

Борьба с даркнет-преступностью представляет собой сложную задачу, требующую комплексного подхода и международного сотрудничества. США и Россия, являясь ведущими игроками в сфере кибербезопасности, применяют различные

¹ © Кольяк А. П., 2025.

стратегии, опираясь на свои национальные законодательства и правоохранительные механизмы. Однако, даже при наличии значительных ресурсов и технологических возможностей, эффективность этих мер ограничена. Одна из главных проблем заключается в юридических аспектах. Законодательство многих стран не успевает адаптироваться к быстро меняющимся реалиям киберпространства. Сбор доказательств в даркнете представляет собой серьезный вызов, так как анонимность пользователей и шифрование трафика значительно затрудняют идентификацию преступников и установление факта совершения преступления. Возникают сложности с доказыванием вины в суде, что часто приводит к тому, что преступники остаются безнаказанными. Существующие международные соглашения и процедуры экстрадиции часто оказываются неэффективными в борьбе с транснациональной преступностью, которая процветает в даркнете. Более того, борьба с даркнетом затрагивает вопросы свободы слова и права на неприкосновенность частной жизни. Необходимо найти баланс между обеспечением безопасности и соблюдением фундаментальных прав человека. Чрезмерно жесткие меры по контролю и мониторингу киберпространства могут привести к нарушению конфиденциальности и подавлению свободы выражения мнений. Поэтому необходим деликатный подход, сочетающий технологические решения с правовыми и этическими аспектами.

Раскрывая подробно правовую базу в США по борьбе с Даркнетом, можно выделить такие нормативный правовые акты, как:

1. Computer Fraud and Abuse Act (CFAA) – Закон о компьютерном мошенничестве и злоупотреблении.
2. Controlled Substances Act – федеральный закон США, принятый в 1970 году. Он регулирует производство, распространение и использование препаратов и химических веществ, которые классифицируются на пять категорий в зависимости от их потенциала для злоупотребления и принятого медицинского применения.

Также помощь в борьбе оказывает федеральное бюро расследований и управление по борьбе с наркотиками в составе Министерства юстиции, которые используют активно операции под прикрытием, что в свою является вхождением в доверие к крупнейшим наркоторговцам, чтобы пресечь каналы поставки.

Говоря о правовой базе РФ выделяют следующие нормативные правовые акты:

1. Уголовный кодекс РФ – статьей 272 предусмотрена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.
2. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 № 115-ФЗ – используется для блокировки криптовалютных операций преступников.

Помощь по борьбе осуществляется также Федеральной службой войск национальной гвардии и Министерством внутренних дел России, которые активно сотрудничают с Федеральной службой безопасности в проведении спецопераций против даркнет-преступников.

Пример борьбы с Даркнетом в США:

1. Операция «Dark HunTor» 2021 года. В ходе операции Dark HunTOR, проведенной правоохранительными органами США, Великобритании, Нидерландов, Австралии, Болгарии, Франции, Германии, Италии и Швейцарии в 2021 г., были арестованы 150 подозреваемых, торговавших нелегальными товарами на DarkMarket. В рамках этой же операции итальянские власти закрыли два даркнет-маркетплейса – Berlusconi и DeepSea.

2. Использование Blockchain-аналитики для отслеживания криптовалютных транзакций. Они изучают, идентифицируют, группируют и интерпретируют данные транзакций блокчейна. В числе анализируемых данных – время и стоимость транзакций, задействованные кошельки, публичные адреса отправителя и получателя.

Пример борьбы с Даркнетом в России:

1. Закрытие «Гидры» в 2022 г. – крупнейшего русскоязычного даркнет-маркетплейса.

2. Управление «К» – подразделение Министерства внутренних дел России, борющееся с преступлениями в сфере информационных технологий.

В заключение, проблема даркнета и связанной с ним преступностью является многогранной и требует сочетания международного сотрудничества, совершенствования законодательства, развития новых технологий мониторинга и расследования киберпреступлений, а также повышения гражданской грамотности в вопросах кибербезопасности. Только комплексный подход позволит эффективно противодействовать угрозам, исходящим из этой скрытой сети, и создать более безопасное информационное общество. Это должно включать не только совершенствование технических средств детектирования и пресечения преступной деятельности, но также пропаганду ответственного пользования интернетом, программы образования и обучения для правоохранительных органов, а также постоянное совершенствование международного законодательства в области киберпреступности. Задача сложная, многоаспектная, и ее решение требует коллективных усилий на глобальном уровне.

Список литературы

1. Choudhury, A. R. Darknet and Cybercrime: A Comprehensive Analysis. Springer. 2021.
2. Dolliver, D. S. Evaluating Drug Trafficking on the Tor Network. Journal of Drug Issues 2015, 45(4), 508-520.
3. Department of Justice Office of Public Affairs FOR Tuesday, September 22, 2020.
4. International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and

over \$6.5 Million URL: <https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170>.

5. Липин Э. Э. Проблема борьбы с преступлениями в интернет-пространстве на примере даркнета / Э. Э. Липин, Г. Д. Дроздов. – Текст : непосредственный // Молодой ученый. – 2020. – № 50 (340). – С. 270–272.

6. Мазур А. А. Актуальные проблемы предупреждения преступности в социальной сети Даркнет // Вестник РУК. 2018. №3 (33).

7. Гонов Ш. Х., Милованов А. В. Актуальные вопросы противодействия преступности в сети даркнет // Полицейская и следственная деятельность. 2021. № 1.

Колышкин М. Л.¹,

курсант института подготовки

сотрудников информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Куликов В. Н.,

старший преподаватель

кафедры иностранных языков

Московского университета МВД России имени В.Я. Кикотя

КИБЕРГИГИЕНА: КАК ПОВЫСИТЬ ОСВЕДОМЛЕННОСТЬ ОБЩЕСТВА В БОРЬБЕ С КИБЕРУГРОЗАМИ

В современном мире, где цифровые технологии проникли во все сферы жизни, вопросы кибербезопасности становятся как никогда актуальными. Кибергигиена – это набор правил и практик, направленных на защиту персональных и корпоративных данных от киберугроз. Ее можно сравнить с личной гигиеной: если не соблюдать базовые меры предосторожности, риск стать жертвой мошенников или вредоносных программ значительно возрастает.

С каждым годом киберпреступность становится все более изощренной. По данным исследований, только в 2023 г. ущерб от кибератак в мире превысил \$ 8 трлн, а к 2025 г. эта цифра может удвоиться. При этом жертвами злоумышленников становятся не только крупные компании, но и обычные пользователи, которые пренебрегают элементарными правилами безопасности [2].

Цель этой статьи – рассказать о ключевых угрозах в интернете и объяснить, как защитить себя от них с помощью простых, но эффективных мер кибергигиены.

Основные угрозы в интернете

1. Вредоносное ПО (вирусы, трояны, ransomware).

Одна из самых распространенных угроз – вредоносные программы, которые могут попасть на устройство через скачанные файлы, фишинговые письма или даже посещение подозрительных сайтов. Вирусы способны не только повредить систему, но и похитить конфиденциальные данные, такие как пароли, банковские реквизиты или личные фото. Особенно опасен ransomware (программы-вымогатели), которые шифруют файлы и требуют выкуп за их разблокировку.

2. Фишинг и социальная инженерия [1].

Фишинг – это мошеннические схемы, при которых злоумышленники выдают себя за доверенные организации (банки, соцсети, госучреждения) и выманивают у пользователей логины, пароли или деньги. Такие атаки часто происходят через поддельные письма, SMS или даже звонки. Социальная инженерия идет дальше: преступники изучают жертву в соцсетях, втираются в доверие и манипулируют, чтобы получить доступ к аккаунтам или деньгам.

¹ © Колышкин М. Л., 2025.

3. Кража личных данных.

Утечки данных случаются регулярно: взламывают базы почтовых сервисов, соцсетей и даже государственных учреждений. Если злоумышленники получают доступ к вашим персональным данным (паспорт, ИНН, номер телефона), они могут оформить кредит на ваше имя, провести мошенническую сделку или шантажировать вас.

4. Небезопасные Wi-Fi сети [3].

Публичные Wi-Fi в кафе, аэропортах или торговых центрах часто не защищены шифрованием. Злоумышленники могут перехватывать трафик и получать доступ к вашим паролям, переписке или банковским операциям. Особенно рискованно в таких сетях вводить логины и платежные данные.

5. Угрозы в социальных сетях и мессенджерах.

Мошенники создают фейковые профили, рассылают спам и вредоносные ссылки, а также используют методы социальной инженерии, чтобы обмануть пользователей. Например, могут написать от имени друга с просьбой «срочно перевести деньги» или предложить «выгодный заработок», который на деле оказывается финансовой пирамидой.

Основные принципы кибергигиены:

1. Надежные пароли и их защита

Используйте сложные пароли длиной не менее 12 символов, сочетающие буквы (включая заглавные), цифры и специальные знаки. Никогда не применяйте один и тот же пароль для разных сервисов – при утечке данных это подвергнет риску все ваши аккаунты. Оптимальное решение – менеджер паролей (LastPass, Bitwarden, KeePass), который не только хранит, но и генерирует надежные комбинации. Особо важные аккаунты (банкинг, почта) защитите дополнительной двухфакторной аутентификацией (2FA) через SMS, приложение или аппаратный ключ.

2. Регулярное обновление программ.

Все установленные программы, операционные системы и антивирусы должны своевременно обновляться. Большинство обновлений содержат критические исправления уязвимостей, которыми активно пользуются хакеры. Включите автоматическое обновление там, где это возможно, и не откладывайте установку патчей. Особое внимание уделяйте браузерам, так как они являются основным каналом для кибератак.

3. Осторожность с электронной почтой и ссылками.

Фишинг остается одним из самых распространенных методов атак. Никогда не открывайте вложения и не переходите по ссылкам в письмах от неизвестных отправителей, даже если они выглядят официально. Проверяйте адрес отправителя (часто он отличается на 1–2 символа от настоящего), не вводите логины и пароли на сайтах, открытых через email. Банки и госучреждения никогда не просят прислать пароли или данные карт по почте.

4. Защита личных данных.

Минимизируйте размещение конфиденциальной информации в открытом доступе. В социальных сетях ограничьте круг лиц, которые могут видеть ваши пер-

сональные данные, фотографии и геолокацию. Никогда не публикуйте сканы документов, билетов или банковских карт – даже закрашенные цифры можно восстановить с помощью специальных программ. Используйте псевдонимы там, где это возможно.

5. Безопасность устройств.

Все гаджеты должны быть защищены PIN-кодом, графическим ключом или биометрией. Установите антивирусное ПО даже на смартфон – мобильные устройства сегодня не менее уязвимы, чем компьютеры. Отключайте Bluetooth и NFC, когда они не используются – через них тоже возможен взлом. Для рабочих и личных устройств используйте шифрование диска (BitLocker, FileVault).

6. Работа с публичными Wi-Fi сетями

Открытые сети в кафе, аэропортах или отелях крайне опасны – злоумышленники могут перехватывать трафик и получать доступ к вашим данным. Если необходимо воспользоваться публичным Wi-Fi, обязательно подключите VPN (NordVPN, ExpressVPN), который зашифрует соединение. Никогда не вводите пароли и не совершайте платежи в таких сетях без защиты.

7. Резервное копирование данных.

Регулярно создавайте копии важных файлов на внешнем жестком диске или в облачном хранилище с надежным шифрованием (Backblaze, iDrive). Это защитит вас от потери данных при ransomware-атаке, поломке устройства или краже. Проверьте, чтобы бэкапы делались автоматически и хранились в нескольких местах.

8. Критическое мышление онлайн.

Не доверяйте слишком выгодным предложениям («iPhone за 1 рубль», «быстрый заработок 100 000 в день»), подозрительным сайтам и сообщениям с просьбой перевести деньги, даже если они приходят от знакомых (их аккаунт мог быть взломан). Проверяйте информацию в официальных источниках, не скачивайте программы с сомнительных сайтов и всегда читайте отзывы перед установкой приложений.

Соблюдение этих принципов не требует специальных технических знаний, но значительно повышает вашу цифровую безопасность. Кибергигиена должна стать такой же привычкой, как мытье рук – регулярной и неотъемлемой частью жизни в цифровую эпоху. Начиная с малого: сегодня смените простые пароли на сложные, завтра установите менеджер паролей, послезавтра – включите двухфакторную аутентификацию. Постепенно эти действия войдут в привычку и создадут надежный барьер против большинства киберугроз.

Что делать в случае взлома? [4]

Обнаружив, что ваш аккаунт или устройство взломаны, важно действовать быстро и последовательно. Вот подробный план действий, который поможет минимизировать ущерб и восстановить контроль:

1. Немедленно смените пароли.

Первое и самое важное – как можно быстрее измените пароль взломанного аккаунта. Если доступ к аккаунту уже заблокирован (злоумышленник поменял пароль), используйте функцию восстановления через привязанную почту или те-

лефон. Для важных сервисов (почта, соцсети, банкинг) установите новый сложный пароль, который вы нигде не использовали ранее. Немедленно смените и пароли на других аккаунтах, где применялся аналогичный или похожий пароль – хакеры часто проверяют украденные данные на разных сервисах.

2. Отключите подозрительные устройства и сессии.

Во многих сервисах (Google, Facebook, ВКонтакте и др.) есть функция просмотра активных сеансов. Проверьте список устройств, с которых выполнен вход, и завершите все подозрительные сессии (особенно те, которые вы не узнаете или которые находятся в незнакомых локациях). В мессенджерах типа Telegram проверьте активные сеансы в настройках и закройте неизвестные подключения.

3. Включите двухфакторную аутентификацию.

Если вы еще не использовали 2FA, немедленно подключите ее для всех важных аккаунтов. Это может быть код из SMS, приложения (Google Authenticator, Microsoft Authenticator) или аппаратный ключ безопасности. Даже если хакер узнает ваш пароль, без второго фактора он не сможет войти. Обновите резервные коды для восстановления и храните их в надежном месте.

4. Проверьте настройки аккаунта и подписки.

Злоумышленники часто меняют настройки профиля (привязанную почту, телефон, резервные адреса), чтобы сохранить доступ. Проверьте, не добавлены ли неизвестные email или номера для восстановления. Посмотрите правила пересылки писем в почте – хакеры могут настроить переадресацию вашей переписки. В соцсетях проверьте, не были ли созданы дополнительные админы или приложения с доступом к аккаунту.

5. Оповестите контакты и отмените финансовые операции.

Если взломаны соцсети или мессенджеры, предупредите друзей и коллег – от вашего имени могли рассылаться мошеннические сообщения с просьбой перевести деньги или перейти по вредоносным ссылкам. При взломе банковского аккаунта или электронного кошелька немедленно позвоните в поддержку банка, заблокируйте карты и отмените подозрительные транзакции. Попросите перевыпустить карты, если есть вероятность, что данные могли быть скомпрометированы.

6. Проверьте устройства на вирусы и шпионское ПО.

Проведите полное сканирование всех устройств, с которых вы заходили во взломанный аккаунт, с помощью надежного антивируса (Kaspersky, Bitdefender, Malwarebytes). Особое внимание уделите подозрительным приложениям, которые могли быть установлены без вашего ведома. На смартфонах проверьте разрешения приложений – некоторые вредоносные программы маскируются под безобидные утилиты, но имеют доступ к вашим сообщениям и паролям.

7. Подайте жалобу в поддержку сервиса.

Почти все крупные платформы (Google, Facebook, Apple и др.) имеют процедуру восстановления взломанных аккаунтов. Официальная жалоба через форму поддержки часто помогает вернуть контроль, особенно если предоставить доказательства владения аккаунтом (старые пароли, данные привязанной карты,

скриншоты прошлых входов). Для банковских и финансовых сервисов жалобу лучше дублировать телефонным звонком.

8. Сообщите о взломе в правоохранительные органы.

Если в результате взлома вы понесли финансовые потери (списаны деньги, оформлены кредиты), или если злоумышленники получили доступ к особо конфиденциальным данным (паспортные данные, интимные фото), необходимо написать заявление в киберполицию. Сохраните все доказательства – скриншоты, переписку, номера кошельков, на которые переводились деньги. В России можно обратиться через сайт МВД России или портал Госуслуг.

9. Проанализируйте причину взлома и усильте защиту.

После восстановления контроля важно понять, как произошел взлом: через фишинг, утечку паролей, уязвимость в программе или другую причину. Это поможет избежать повторения ситуации. Обновите все пароли, установите менеджер паролей, проверьте компьютер на keylogger'ы (программы, записывающие нажатия клавиш), будьте осторожнее с подозрительными ссылками и письмами.

10. Предупредите последствия для репутации.

Если взломаны соцсети или почта, где хранилась важная переписка, подумайте, как это может повлиять на вашу репутацию. Возможно, стоит предупредить партнеров или работодателя о возможных странных сообщениях от вашего имени. В некоторых случаях имеет смысл временно деактивировать аккаунт, пока не будет восстановлен полный контроль.

В современном мире, где большая часть нашей жизни переместилась в онлайн, соблюдение правил кибергигиены перестало быть рекомендацией – это обязательное условие безопасности. Как мы ежедневно чистим зубы и моем руки, так же регулярно нужно проверять настройки аккаунтов, обновлять пароли и следить за цифровой чистотой своих устройств. Киберпреступники постоянно совершенствуют свои методы, но большинство атак можно предотвратить, следуя простым принципам: использованию надежных паролей, двухфакторной аутентификации, осторожности с письмами и ссылками, регулярному обновлению программного обеспечения. Важно помнить, что безопасность в интернете – это не разовое действие, а постоянный процесс. Если же взлом все-таки произошел, главное – не паниковать, а оперативно действовать по четкому плану: сменить пароли, отключить подозрительные сессии, проверить устройства на вирусы и при необходимости обратиться в поддержку сервиса или правоохранительные органы. Кибергигиена – это ответственность каждого пользователя. Начиная с базовых мер защиты и заканчивая обучением цифровой грамотности своих близких, мы можем сделать интернет безопаснее для себя и окружающих. Помните: ваша внимательность и дисциплина – самый надежный щит против киберугроз. Внедряйте правила кибергигиены в повседневную жизнь, и цифровое пространство станет значительно комфортнее и безопаснее.

Список литературы

1. Национальная стратегия развития искусственного интеллекта на период до 2030 года (Указ Президента Российской Федерации № 490 от 10.10.2019).
2. Галатенко В. А. (2022). Основы информационной безопасности – М.: Интернет-Университет Информационных Технологий.
3. Петренко С. А., Курбатов В. А. (2021). Кибербезопасность и кибергигиена – СПб.: Питер.
4. Официальный сайт Госуслуги.Кибербезопасность.

Короленко Е. С.¹,

курсант института подготовки

сотрудников для органов

предварительного расследования

Московского университета МВД России имени В.Я.Кикотя

Научный руководитель:

Серебрякова О. М.,

доцент кафедры иностранных языков

Московского университета МВД России имени В.Я. Кикотя,

кандидат филологических наук

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

В связи с возрастающим числом киберугроз в современном цифровом пространстве значимость применения искусственного интеллекта в сфере кибербезопасности становится все более очевидной и неоспоримой. Целью данной статьи является изучение вопроса об интеграции алгоритмов машинного обучения, автоматизированных процессов выявления и противодействия кибератакам, а также осмысления и разрешение этических проблем, возникающих при использовании искусственного интеллекта. На основе анализа существующих методов использования искусственного интеллекта и будущих тенденций развития, исследование демонстрирует, как искусственный интеллект способен трансформировать систему кибербезопасности, предлагая проактивную и адаптируемую стратегию борьбы с кибератаками.

В современном цифровом мире, где технологии становятся все более сложными, а киберугрозы все более утонченными, роль искусственного интеллекта в обеспечении кибербезопасности становится ключевой. Искусственный интеллект внедряется в сферу кибербезопасности с целью не только обнаружения и предотвращения угроз, но и эффективного реагирования на них.

С увеличением масштабов цифровизации и активной интеграции информационных технологий в повседневную жизнь человечество сталкивается с все более значимыми и сложными угрозами в киберпространстве. Фишинговые атаки относятся к числу наиболее распространенных и разрушительных видов киберпреступности.

Киберпреступники постоянно совершенствуют свои методы, делая атаки все более скрытными, целенаправленными и разрушительными. В этом контексте традиционные подходы к обеспечению кибербезопасности, основанные на сигнатурном анализе и ручной аналитике, теряют свою эффективность. Киберпреступники имели возможность легко обойти системы обнаружения, основанные на сигнатурах, изменив код или создав новые варианты вредоносного программного обеспечения, которых еще не было в базе данных. Возникает объективная

¹ © Короленко Е. С., 2025.

необходимость внедрения новых технологий, способных оперативно и точно реагировать на современные угрозы. Одной из таких технологий становится искусственный интеллект, предоставляющий уникальные возможности по анализу большого массива данных, выявлению тенденций и принятию решений в режиме реального времени [1, с. 3819–3828].

С внедрением технологий, обеспечивающих сохранение конфиденциальности, правоохранительные органы в последнее время все чаще сталкиваются с необходимостью увязки кибербезопасности, основанной на искусственном интеллекте, с сохранением конфиденциальности в киберэкосистеме. Конфликт, созданный с помощью искусственного интеллекта, является еще одной серьезной проблемой в области кибербезопасности. Сам по себе искусственный интеллект может быть полезен в области кибербезопасности, но проблемы, связанные с ним, требуют принятия упреждающих мер.

С одной стороны, технологии искусственного интеллекта обеспечивают эффективные решения в области кибербезопасности, а с другой - усиливают защиту от атак. В различных источниках указывается, что у каждого инструмента, включая ИИ, есть как положительные, так и отрицательные стороны.

Организациям и пользователям глобальной интернет сети необходимо найти способы опережать кибератаки. Быстро развивающиеся технологии создают благоприятную почву для создания новых и неожиданных атак. Заказные атаки направлены на использование коммерческой тайны организаций, финансовых данных и стратегической информации. Поэтому важно, чтобы сотрудники службы информационной безопасности использовали искусственный интеллект в качестве стратегического инструмента в своих комплексных планах по кибербезопасности и цифровой защите, чтобы гарантировать долгосрочную защиту в области кибербезопасности.

Искусственный интеллект и машинное обучение по своей сути сложны, и их необходимо проектировать таким образом, чтобы они включали методы совместного обучения, рассуждения, адаптации и запоминания с гарантированной безопасностью и надежностью. В связи с этим возникают некоторые серьезные проблемы, связанные с эвристикой, основанной на ИИ. Более того, такие модели, основанные на искусственном интеллекте и машинном обучении, как правило, должны работать с сильно распределенными и динамичными организационными данными.

Искусственный интеллект представляет собой обширную совокупность методов и алгоритмов, которые позволяют техническим системам имитировать интеллектуальные функции человека, такие как обучение, анализ, прогнозирование и принятие решений.

В сфере кибербезопасности такие технологии используются для анализа сетевой активности, оценки поведения пользователей, обработки текстовой информации и автоматизации ответных мер на инциденты. Ключевую роль в этом процессе играют машинное обучение, обработка естественного языка и поведенческий анализ. Алгоритмы машинного обучения позволяют системам автоматически анализировать большие объемы данных, выявлять аномалии и

прогнозировать возможные кибератаки. Это повышает оперативность реагирования и позволяет предотвращать угрозы до того, как они нанесут ущерб. Технологии машинного обучения также способствуют созданию интеллектуальных систем, способных адаптироваться к новым типам угроз. Системы, оснащенные искусственным интеллектом, могут извлекать опыт из новых данных и в дальнейшем повышать свою эффективность. Это особенно важно в условиях появления новых видов кибератак. Кроме того, искусственный интеллект используется для создания интеллектуальных систем анализа угроз и решения сложных киберпроблем [2, с. 135–147]. Такие системы могут обрабатывать данные в режиме реального времени, выявлять нестандартное поведение пользователей, анализировать сетевой трафик и обнаруживать скрытые угрозы.

Обработка естественного языка, являющаяся еще одним направлением в развитии искусственного интеллекта, находит широкое применение при анализе текстовых данных. С ее помощью можно выявлять признаки социальной инженерии, фишинговых атак, а также осуществлять автоматическое категоризирование информации, поступающей в системы безопасности. Это особенно важно в условиях увеличения объема данных, требующих анализа в кратчайшие сроки [3, с.118–122].

Однако несмотря на многочисленные преимущества искусственного интеллекта в борьбе с фишингом и другими кибератаками, он имеет некоторые недостатки. Основная проблема заключается в том, что системы искусственного интеллекта могут выдавать ложные срабатывания, что может привести к ненужным задержкам в процессе деятельности. Например, системы искусственного интеллекта могут ошибочно идентифицировать действительные электронные письма как фишинговые, что приводит к неэффективности и задержкам. Чтобы уменьшить количество ложных срабатываний и повысить точность обнаружения угроз, алгоритмы искусственного интеллекта должны постоянно обучаться и совершенствоваться. Способность искусственного интеллекта к улучшению своих алгоритмы с течением времени позволяет ему более точно отличать реальные угрозы от безобидных действий. Это снижает вероятность ложных срабатываний и позволяет специалистам по безопасности сосредоточиться на реальных опасностях.

Также важно отметить, что наряду с повышенной киберзащитой, искусственный интеллект также становится инструментом для создания более сложных кибератак.

Злоумышленники могут использовать технологии машинного обучения для создания интеллектуальных и трудных для определения угроз. Чтобы опережать появление новых возможных угрозы, организациям по обеспечению безопасности необходимо проявлять осторожность, поскольку как технологии искусственного интеллекта, так и киберугрозы постоянно развиваются. Эта непрекращающаяся конкуренция между киберпреступниками и охранными фирмами показывает, насколько важно регулярно разрабатывать и совершенствовать решения для обеспечения кибербезопасности на базе искусственного интеллекта.

Необходимо отметить и этический аспект использования искусственного интеллекта. В настоящее время проблемы, связанные с конфиденциальностью, от-

ветственностью за решения искусственного интеллекта, а также за создание конкретных стандартов в данной области регулирования становятся все более актуальными.

Сбалансированный подход к устранению недостатков полностью автоматизированных систем заключается в сочетании функций искусственного интеллекта с качественным управлением со стороны человека. Для понимания сложных ситуаций, принятия обоснованных решений и корректировки мер безопасности в связи с постоянно меняющимися киберугрозами необходим контроль со стороны специалистов. Хотя алгоритмы искусственного интеллекта превосходно обнаруживают подозрительную сетевую активность или попытки фишинга, они имеют тенденцию ошибочно принимать безобидные действия за угрозы - явление, известное как ложные срабатывания [4, с.78–82].

В полностью автоматизированной системе это может привести к сбоям, таким как блокировка законных электронных писем, пользователей или сервисов. Специалисты-аналитики, обладающие знаниями в данной области, могут проанализировать эти действия, чтобы определить, действительно ли они представляют опасность или являются ложными тревогами.

Кроме того, данные, генерируемые системами искусственного интеллекта, должны быть контекстуализированы и интерпретированы людьми. Искусственный интеллект может выявлять поверхностные отклонения и тенденции, но он может не понимать общей картины или мотивов. Грамотный подход к сочетанию функций искусственного интеллекта и человека гарантирует эффективное и этичное применение мощных инструментов для обнаружения киберугроз и реагирования на них [5, с.151–154].

Подводя итог, можно сказать, что использование искусственного интеллекта в сфере кибербезопасности – это огромный шаг вперед в борьбе с киберугрозами. Улучшенные механизмы обнаружения, предотвращения и реагирования на угрозы находятся в пределах досягаемости благодаря способности искусственного интеллекта выявлять сложные закономерности и приспосабливаться к новым опасностям.

Однако применение искусственного интеллекта для обеспечения кибербезопасности – это не простой процесс. Чтобы максимально эффективно использовать искусственный интеллект и минимизировать связанные с ним риски, крайне важно продвигать открытость, ответственность и этичное использование технологий. Комплексные решения в области кибербезопасности потребуют сочетания искусственного интеллекта и человеческих знаний, которые будут приобретать все большее значение по мере развития технологий.

Дальнейшее развитие и внедрение искусственного интеллекта в соответствии с этическими нормами будет в значительной степени способствовать повышению эффективности и адаптивности кибербезопасности в постоянно меняющемся цифровом мире.

Список литературы

1. Mughaid, Ala, Shadi AlZu'bi, Adnan Hnaif, Salah Taamneh, Asma Alnajjar, and Esraa Abu Elsoud. "An intelligent cyber security phishing detection system using deep learning techniques." *Cluster Computing* 25, no. 6 ,2022.
2. Намиот Д. Е., Ильюшин Е. А., Чижов И. В. Искусственный интеллект и кибербезопасность, *International Journal of Open Information Technologies*, 2020.
3. Siddiqui, Md Zeeshan, Sonali Yadav, and Mohd Shahid Husain. "Application of artificial intelligence in fighting against cyber crimes: a review." *Int. J. Adv. Res. Comput. Sci* 9, no. 2 ,2018.
4. Rastogi, Malaika, Anmol Chhetri, and Divyanshu Kumar Singh. "Survey on detection and prevention of phishing websites using machine learning." In *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021.
5. Афанасьева Д. В. Применение искусственного интеллекта в обеспечении безопасности данных. // *Известия Тульского государственного университета*», 2020.

Котцова М. П.¹,

курсант международно-правового факультета

Московского университета МВД России имени В. Я. Кикотя

Научный руководитель:

Хмирова Е. А.,

старший преподаватель кафедры иностранных языков

Московского университета МВД России имени В. Я. Кикотя

РОЛЬ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ В США

Киберпреступность в современных условиях представляет собой одну из наиболее серьезных угроз национальной безопасности, экономическому развитию и общественному порядку. Согласно отчету Интернет-центра жалоб на преступления (Internet Crime Complaint Center, IC3) ФБР за 2023 г., финансовые потери от киберпреступлений в США достигли рекордного показателя в 12,5 миллиардов долларов, что на 22 % превышает аналогичный показатель предыдущего года [2]. При этом было зарегистрировано 880.418 жалоб, что также является историческим максимумом [2]. Особую обеспокоенность вызывает стремительный рост атак программ-вымогателей (ransomware), количество которых увеличилось на 18 % по сравнению с 2022 г. [3]. Трансграничный характер киберпреступности, возможность осуществления атак практически из любой точки мира и сложности в установлении личности правонарушителей создают значительные препятствия для эффективного противодействия данному виду противоправной деятельности в рамках отдельно взятого государства.

Проблематика международного сотрудничества в борьбе с киберпреступностью находится в фокусе внимания ведущих зарубежных ученых. Значительный вклад в разработку данной темы внесли такие исследователи, как Томас Холт (Мичиганский государственный университет), специализирующийся на криминологических аспектах киберпреступности, Анита Лаворгна (Болонский университет), изучающая транснациональную организованную киберпреступность, Дэвид Деками-Хету (Университет Монреаля), фокусирующийся на социальных измерениях киберпреступности, Марко Романья (Лейденский университет), исследующий киберкриминологию, и Фернандо Миро (Университет Мигеля Эрнандеса), разрабатывающий концепции кибербезопасности и предупреждения киберпреступлений [1]. Их научные работы освещают различные аспекты международного сотрудничества в противодействии киберпреступности, включая правовые, организационные и технические аспекты данной проблематики.

Анализ статистических данных правоохранительных органов США свидетельствует о беспрецедентном росте киберпреступности в последние годы. Согласно отчету ФБР, в 2023 г. общий финансовый ущерб от киберпреступлений

¹ © Котцова М. П., 2025.

достиг рекордного показателя в 12,5 миллиардов долларов, что на 22 % превышает показатель 2022 г. [3]. При этом количество зарегистрированных жалоб на киберпреступления составило 880.418, что также является историческим максимумом [4].

Особую обеспокоенность вызывает значительный рост инвестиционного мошенничества, которое в 2023 г. причинило ущерб в размере 4,57 миллиарда долларов, что на 38 % больше по сравнению с предыдущим годом [4]. При этом потери от мошенничества с криптовалютными инвестициями составили 3,94 миллиарда долларов, увеличившись на 53 % по сравнению с 2022 г. [3]. Данная тенденция свидетельствует о том, что киберпреступники активно адаптируются к новым технологическим реалиям и используют возрастающую популярность криптовалют для осуществления противоправной деятельности.

Компрометация деловой электронной почты (Business Email Compromise, BEC) также остается серьезной проблемой. В 2023 г. было зарегистрировано 21.489 жалоб на BEC, а финансовые потери составили 2,9 миллиарда долларов, что на 7,4 % больше по сравнению с 2022 г. [3]. Данный вид киберпреступлений характеризуется высокой степенью изощренности и часто целенаправленно атакует конкретные организации, что осложняет процесс выявления и предотвращения таких атак.

Наблюдается существенный рост атак программ-вымогателей (ransomware). По данным ФБР, в 2023 г. количество жалоб на атаки программ-вымогателей увеличилось на 18 % по сравнению с предыдущим годом, достигнув 2.825 [3]. При этом финансовые потери от таких атак выросли на 74 % по сравнению с 2022 г. [4]. Особую тревогу вызывает то, что, согласно отчету ФБР, пять ведущих групп программ-вымогателей, атакующих США, являются русскоязычными, включая печально известные Lockbit и Blackcat/APLHV.

Наиболее распространенным типом киберпреступлений в 2023 г. был фишинг. Было зарегистрировано более 298 тыс. жалоб на фишинговые схемы, что составляет примерно 34 % от всех зарегистрированных жалоб [3]. Фишинговые атаки становятся все более изощренными и часто представляют собой первый этап более сложных многоступенчатых атак.

Важно отметить, что реальный масштаб киберпреступности в США и связанный с ней финансовый ущерб, вероятно, значительно выше, поскольку многие киберпреступления остаются незарегистрированными. По оценкам экспертов, только 3 из 1000 киберинцидентов, о которых сообщается в ФБР, заканчиваются арестом [4]. Такой низкий показатель раскрываемости свидетельствует о сложности расследования киберпреступлений и привлечения виновных к ответственности.

Ключевой особенностью киберпреступности является ее транснациональный характер. Расследование одного киберпреступления часто требует взаимодействия правоохранительных органов и судебных систем нескольких стран [2]. Например, для ареста лидера одной киберпреступной группировки, атаковавшей более 100 финансовых учреждений в более чем 40 странах, потребовалось со-

трудничество ФБР с правоохрательными органами пяти разных стран, частными компаниями в сфере кибербезопасности и Европейским полицейским агентством (EUROPOL) [3].

Таким образом, современное состояние киберпреступности в США характеризуется значительным ростом масштабов и финансового ущерба, усложнением методов и средств совершения преступлений, а также их транснациональным характером, что обуславливает необходимость развития и укрепления международного сотрудничества в данной сфере.

Международное сотрудничество США в борьбе с киберпреступностью осуществляется через правоохрательные органы, международные организации, государственно-частное партнерство и выполнение положений международных соглашений. Федеральное бюро расследований (ФБР) играет ключевую роль, включая деятельность Интернет-центра жалоб на преступления (IC3), который анализирует данные о киберпреступлениях и передает их правоохрательным органам. ФБР также взаимодействует с зарубежными представителями в посольствах США.

Киберкомандование США отвечает за военные кибероперации и защиту сетей, сотрудничая с аналогичными структурами других стран. США участвуют в работе международных организаций, таких как Комиссия ООН по предупреждению преступности (ССРСJ), Организация по безопасности и сотрудничеству в Европе (ОБСЕ), а также Организация американских государств (ОАГ). ОБСЕ разрабатывает меры укрепления доверия для снижения конфликтов, а ОАГ создала портал для обмена информацией между экспертами по киберпреступности.

США активно участвуют в сети контактных пунктов 24/7 Совета Европы и ИНТЕРПОЛа для оперативного обмена данными. В рамках Европола они являются членом Совместной целевой группы по борьбе с киберпреступностью (J-CAT), которая координирует действия против угроз. Также США входят в Глобальный форум по киберэкспертизе (GFCE), где происходит обмен исследованиями и опытом.

Государственно-частное партнерство играет важную роль: США сотрудничают с компаниями, такими как Microsoft и Symantec, для реагирования на инциденты. Примером успешного сотрудничества стала операция по ликвидации ботнета Emotet в 2021 г. с участием правоохрательных органов нескольких стран.

В условиях стремительного роста киберпреступности и усложнения ее форм и методов, развитие международного сотрудничества приобретает критическое значение для эффективного противодействия данному виду преступности. Анализ существующих проблем и вызовов позволяет определить ряд перспективных направлений развития международного сотрудничества США в борьбе с киберпреступностью.

Одним из ключевых направлений являются расширение и углубление многостороннего сотрудничества. Это предполагает увеличение числа участников Будапештской конвенции, разработку новых многосторонних соглашений и механизмов сотрудничества, а также укрепление существующих форматов взаимодействия. Особое внимание следует уделить привлечению к сотрудничеству

таких крупных государств, как Россия и Китай, которые не являются участниками Будапештской конвенции.

Приоритетным направлением является восстановление диалога между США и Россией по кибервопросам. Отношения между двумя странами имеют ключевое значение для всей экосистемы киберполитики и дипломатии, поскольку они являются одними из наиболее развитых кибердержав. Несмотря на взаимные обвинения и разногласия, США и Россия могли бы стремиться к заключению реалистичного и ограниченного по объему соглашения, например, по предотвращению опасной военной деятельности в киберпространстве, подобно Соглашению о предотвращении инцидентов в открытом море 1972 г.

Обсуждение глобальной конвенции о киберпреступности представляет собой еще одно перспективное направление. Данный вопрос должен рассматриваться в рамках ООН, где существует механизм для обсуждения глобального сотрудничества в борьбе с киберпреступностью – межправительственная группа экспертов по киберпреступности.

Для упрощения атрибуции киберинцидентов, которая является одной из ключевых проблем в борьбе с киберпреступностью, правительства и глобальное техническое сообщество могли бы разработать улучшения и обновления для основных интернет-протоколов. Это поможет проверять соблюдение принципов международного права, таких как невмешательство во внутренние дела других государств, и возлагать на государства большую ответственность за то, что происходит в их киберпространстве.

В долгосрочной перспективе целесообразным представляется создание международного киберсуда или аналогичного органа. В связи с растущим числом обвинений в кибератаках между государствами и сложностью технической атрибуции было бы полезно создать независимый, международный киберсуд или метод арбитража, который занимался бы только кибер-конфликтами на правительственном уровне и который признавался и уважался бы всеми сторонами [5]. В таком суде одна сторона могла бы представить доказательства того, что она подверглась хакерской атаке, обвиняемая сторона могла бы утверждать, что она не стоит за атакой, а независимые, квалифицированные эксперты пытались бы проверить точность этих утверждений.

Ограничение автономного кибероружия также представляется важным направлением развития международного сотрудничества. Кибероружие, работающее без участия человека, должно быть запрещено. Атаки часто проходят через компьютеры в невиновных третьих странах, информация граждан которых подвергается риску из-за автономного кибероружия, которое не соблюдает национальные границы [6]. Заседание Группы правительственных экспертов ООН по летальным автономным системам оружия, проведенное в ноябре 2017 г. в рамках Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, было первым официальным заседанием по таким видам оружия и является хорошей площадкой для принятия конкретных мер по укреплению кодекса поведения [5].

Список литературы

1. Holt, T. J. A professor in the School of Criminal Justice at Michigan State University whose research focuses on computer hacking, malware, and the role of the Internet in facilitating all manner of crime and deviance / T. J. Holt // Criminal Investigations and Network Analysis Center. – 2023. – URL: <https://cina.gmu.edu/people/thomas-holt/> (date of access: 07.04.2025).
2. Federal Bureau of Investigation. Internet Crime Report 2023 / FBI Internet Crime Complaint Center (IC3). – Washington, D.C., 2023. – 45 p.
3. Federal Bureau of Investigation. Cybercrime Investigation Statistics / FBI Cyber Division. – Washington, D.C., 2023. – 32 p.
4. Federal Bureau of Investigation. Ransomware Trends Report / FBI Cyber Division. – Washington, D.C., 2023. – 28 p.
5. Federal Bureau of Investigation. Analysis of Cyber Threats and Financial Losses / FBI Internet Crime Complaint Center (IC3). – Washington, D.C., 2023. – 53 p.
6. Federal Bureau of Investigation. Annual Statistical Report on Cyber Complaints / FBI Internet Crime Complaint Center (IC3). – Washington, D.C., 2023. – 67 p.

Кравченко В. И.¹,
курсант 932 взвода
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Куликов В. Н.,
старший преподаватель
кафедры иностранных языков
Московского университета МВД России имени В.Я. Кикотя

МЕТОДЫ ОТСЛЕЖИВАНИЯ ТРАНЗАКЦИЙ КРИПТОВАЛЮТ ПРИ РАССЛЕДОВАНИИ ФИНАНСИРОВАНИЯ ПРЕСТУПНЫХ ОРГАНИЗАЦИЙ

С ростом цены популярных криптовалют и, как следствие, интереса к технологии «блокчейн» правоохранительные органы разных стран столкнулись с новыми вызовами и угрозами. Являясь децентрализованной и декларативно анонимной системой финансовых переводов, транзакции криптовалют весьма скоро раскрыли свой деструктивный потенциал.

Такие криптовалюты, как Bitcoin, стали распространенными меновыми эквивалентами при осуществлении сделок о покупке незаконных товаров и услуг, в том числе размещенных в Darknet. С развитием технологий блокчейна в новых криптовалютах, а равно и сервисов для работы с криптокошельками, возникла и практика использования криптовалют различного рода организованными преступными группировками (ОПГ) в России и по всему миру.

Батоев В. Б. и Семенчук В. В. характеризуют криптовалюту как то, чему требуются регуляция со стороны государства, чему должны способствовать научные исследования [6].

Террористические организации по всему миру отказались от использования традиционных средств платежа в пользу криптовалют [4, с. 129]. Также осуществляющие рэкёт высоко оценивают возможности криптовалют [4, с. 130–133].

Так, зафиксировано использование криптовалют при финансировании терроризма, отмывании денег и распространении фальшивых купюр. В России была раскрыта трансграничная группа криптомошенников, осуществлявшая нелегальные переводы за рубеж [1]. Росфинмониторинг зафиксировал случаи использования криптовалют для финансирования террористических организаций [2]. Также выявлена преступная сеть, продававшая поддельные деньги в даркнете за цифровые активы, что привело к аресту 24 ее участников [3].

Таким образом, возникает необходимость в разработке методологии, позволяющей правоохранительным органам разных стран отслеживать транзакции криптовалют. Мы предлагаем следующую классификацию кластеров общих методов:

1. Использование уязвимостей блокчейн.

¹ © Кравченко В. И., 2025.

2. Сотрудничество с криптобиржами.
3. Использование уязвимостей криптобирж.
4. Работа с провайдерами.
5. Социальная инженерия.

А также частный метод для отслеживания транзакций криптовалют преступных организаций:

6. Использование агентов внутри организации.

Они обусловлены спецификой тактики противодействия преступным организациям. В первую очередь налаженность инфраструктуры и мощная корпоративная культура различного рода экстремистских, террористических сообществ, ОПГ становится проблемой. В случае с преступлениями, совершенными частными лицами, расследование ведется по стандартным процедурам, тогда как противодействие организованным группировкам осложняется их устойчивой структурой, системой конспирации и распределением ролей. Преступные сообщества обладают развитой инфраструктурой, что затрудняет их выявление и ликвидацию, требуя более сложных методов расследования и координации между правоохранительными органами.

Несмотря на то что криптовалюты заявлены как анонимное средство платежа, в силу устройства технологии «блокчейн» это не так.

Каждый блок содержит ссылку на предыдущий блок. Это служит подтверждению истинности блока, так как незначительное изменение блока, попытка внести недостоверные данные создадут новую цепочку хешей таким образом, что это не останется незамеченным [5, с. 9–11].

В UTXO-моделях, таких как Bitcoin, каждая транзакция содержит ссылки на все входы и формирует новый выход, который именуется UTXO, что служит подтверждению возможности осуществлению транзакции. Транзакция содержит информацию о публичном ключе получателя и цифровую подпись отправителя. При анализе блоков мы можем выявить связи между переводами достоверно определять и отождествлять агента с самим собой.

В балансных моделях (например, Ethereum и криптовалюты на его архитектуре) каждый блок содержит информацию о количестве средств в активных кошельках, что значительно упрощает анализ, ведь количество изменяющихся средств в кошельке служит дополнительным индикатором, создавая более комфортные условия отслеживания движения криптовалютной массы.

Однако существуют менее распространенные, но более анонимные криптовалюты, подтверждающие подлинность транзакции иными методами. В таких случаях отслеживание транзакций заметно усложняется, но также остается возможной.

Для создания помех отслеживанию переводов были изобретены транзакционные миксеры, суть которых в создании новых транзакций автоматически в большом количестве, что удлиняет цепочку блоков. Современные сервисы анализа транзакций позволяют нивелировать действие миксеров.

Хотя анализ цепочек блоков позволяет отслеживать транзакции криптовалют, сам по себе он не раскрывает личности отправителя перевода и его адресата. Во время данного анализа правоохранительные органы могут узнать информацию о

псевдониме, размере перевода, времени перевода. Для установления личности требуется отдельная работа.

Но существование более защищенных криптовалют требует поиск новых уязвимостей. Это похоже на эволюцию крепостей и осадных орудий в средневековье – как бы мы не старались соорудить все более мощную пушку, преступники все более утолщают и усложняют стены. Так, при легализации (отмывании) наркодоходов, контрабанде и незаконном сбыте наркотических средств в отдельных странах Латинской Америки и Карибского бассейна преступные организации используют «Dah», «Monero», «ZCash» [8].

Сотрудничество государственных органов с криптовалютными биржами в целях отслеживания транзакций, связанных с организованной преступностью, становится важным направлением в борьбе с финансовыми преступлениями. Криптовалюты, благодаря своей децентрализованной природе, предоставляют преступным группировкам возможности для анонимных переводов и отмывания денежных средств. Однако современные механизмы регулирования, в том числе требования по идентификации пользователей (KYC) и мониторинг подозрительных операций (AML) [7], позволяют государствам получать доступ к данным о транзакциях и выявлять преступные схемы.

Многие государства заключают соглашения с криптобиржами о предоставлении информации правоохранным органам в случае подозрительной активности. Биржи, зарегистрированные в юрисдикциях с жестким регулированием, обязаны вести учет данных клиентов и предоставлять их по запросу уполномоченных органов. Кроме того, развитие технологий анализа блокчейна, таких как Chainalysis и CipherTrace, позволяет государствам эффективно отслеживать передвижение цифровых активов, даже если они проходят через несколько анонимизированных транзакций. Это затрудняет использование криптовалют для финансирования преступной деятельности.

Несмотря на усилия по регулированию, остаются вызовы, связанные с биржами, работающими в странах с менее строгими требованиями к комплаенсу. Некоторые площадки не требуют верификации пользователей или допускают операции через децентрализованные протоколы, что усложняет процесс выявления реальных владельцев кошельков. В таких случаях правоохранные органы прибегают к международному сотрудничеству, санкциям против нерегулируемых платформ и технологическим методам деанонимизации, позволяющим связывать адреса криптовалютных кошельков с реальными лицами.

Криптовалютные биржи стали одной из главных мишеней для киберпреступников из-за их высокой ликвидности и значительных объемов хранимых активов. Хакеры используют различные методы атак, включая фишинг, взлом учетных записей, эксплойты уязвимостей программного обеспечения и перехват данных API. Одним из самых известных случаев стал взлом Mt. Gox в 2014 г., когда из-за утечки ключей было похищено около 850 000 BTC. Впоследствии хакеры неоднократно атаковали крупные платформы, например, в 2018 г. биржа Coincheck потеряла криптоактивы на сумму более \$500 млн из-за недостаточной защиты горячих кошельков [9].

Одной из ключевых проблем безопасности криптобирж является недостаточный уровень шифрования и хранения данных. Многие платформы хранят значительные объемы средств в горячих кошельках, что делает их уязвимыми перед атаками. Взломщики могут использовать недостатки в системе авторизации, перехватывать сессии пользователей или внедрять вредоносный код. Кроме того, в некоторых случаях злоумышленники получают доступ к биржам через инсайдеров или социальную инженерию, что позволяет обойти даже многофакторную аутентификацию.

Правоохранительные органы все чаще используют уязвимости криптовалютных бирж для отслеживания преступной деятельности, выявления незаконных финансовых потоков и борьбы с отмыванием денег. Одним из ключевых методов является анализ транзакционных данных, утечек информации и слабых мест в системе безопасности бирж.

В случае, если запросы отправляются по протоколу HTTP, провайдер может перехватить содержимое запроса, являясь MITM. Однако распространение HTTPS лишает правоохранительных органов возможности получить содержимое запроса, так как сообщение шифруется на стороне клиента и дешифруется только на стороне сервера. В то же время данные: IP клиента, IP сервера, имя домена, время отправки запроса, продолжительность соединения – остаются доступными для провайдера.

Практика использовать провайдеров для установления личности в сети Интернет является весьма распространенной. Так, например, это используется при установлении личности владельцев Telegram-каналов. Метод является достаточно тривиальным, но требует времени.

Возможен и вариант с использованием публичных WiFi-сетей для перехвата запросов [10]. Этот вариант относится к данной категории непрямо, но духом. В таком случае мы просто переносим роль провайдера на владельца публичной WiFi-сети.

Очевидно, такой способ как работа с провайдерами не является возможным в случаях, если провайдер находится в юрисдикции другой страны. В таком случае требуются дополнительные условия его использования, а главное – международное сотрудничество.

Более того, не все страны в принципе обязуют провайдеров сотрудничать с правоохранительными органами, ведя журналирование HTTP/HTTPS запросов.

Более универсальным, но в то же время непредсказуемым методом установления личности является применение Osint, что может занимать еще больше времени или в принципе не сработать в случае, если злоумышленники действительно хорошо подготовлены.

Речь идет о поиске адресов биткоин-кошельков в открытом доступе и сопоставлении их с данными аккаунтов на различных веб-сайтах.

Например, владелец биткоин-кошелька может отправлять по разным причинам адрес своего биткоин-кошелька в мессенджерах, сайтах знакомств и во многие иные ресурсы, к которым есть доступ. Данные, такие как имя пользователя, могут применяться на разных сайтах одним и тем же человеком раз за разом, что дает почву для деанонимизации [10].

Мы можем провоцировать злоумышленника на предоставление дополнительных данных. Так или иначе, данный метод подразумевает использовать недостатки не самих систем, защищающих правонарушителей, но недостатки самих правонарушителей.

Использование агентов под прикрытием является эффективным методом отслеживания транзакций криптовалют при расследовании финансирования преступных организаций. Внедряясь в такие группы, агенты могут собирать ключевую информацию о механизмах отмывания денег и идентифицировать участников незаконных схем. Например, в 2021 г. сотрудники Налогового управления США (IRS) создали профиль под псевдонимом «Mr. Coins» на платформе LocalCryptos.com, выдавая себя за трейдера криптовалют. Это позволило им выйти на предполагаемого наркоторговца, который отправил более 180 000 долларов наличными в обмен на биткоины. В результате операции подозреваемый был арестован и предъявлены обвинения в отмывании денег и торговле наркотиками [11].

Представленные методы отслеживания транзакций являются активно используемыми практиками для органов защиты правопорядка разных стран мира, включая в Россию. Разработка новых методов является важной задачей последующих исследований. Но даже на данном этапе правоохранительные органы обладают необходимыми инструментами, их развитие будет способствовать раскрытию преступлений, связанных с криптовалютами.

Список литературы

1. Freedom Broker. Трансграничную группировку криптомошенников раскрыли в России. [Электронный ресурс]. Режим доступа URL: <https://24.kz/ru/news/in-the-world/672101-transgranichnuyu-gruppirovku-kriptomoshennikov-raskryli-v-rossii>. (дата обращения: 02.04.2025).
2. ТАСС. Росфинмониторинг фиксирует отдельные случаи использования криптовалюты в целях терроризма. [Электронный ресурс]. Режим доступа URL: <https://tass.ru/politika/16374407>. (дата обращения: 02.04.2025).
3. РАПСИ. Арестованы 24 члена ОПГ, торговавшие в Darknet фальшивыми деньгами. [Электронный ресурс]. Режим доступа URL: https://rapsinews.ru/judicial_news/20231107/309361852.html. (дата обращения: 02.04.2025).
4. Pieroni C. La Crypto Nostra: How Organized Crime Thrives in the Era of Cryptocurrency //North Carolina Journal of Law & Technology. – 2018. – Т. 20. – №. 5. – С. 111.
5. Collins J. Crypto, crime and control //Cryptocurrencies as an enabler of organized crime, Global Initiative Against Transnational Organized Crime. – 2022.
6. Батоев В. Б., Семенчук В. В. Использование криптовалюты в преступной деятельности: проблемы противодействия //Труды Академии управления МВД России. – 2017. – №. 2 (42). – С. 9–15.

7. Черявко Е. Д. Использование цифровых технологий организованной преступностью //Новизна. Эксперимент. Традиции. – 2023. – Т. 9. – №. 3 (23). – С. 68–75.

8. Земцова С. И., Суров О. А. Противодействие транснациональной организованной преступности в сфере незаконного оборота наркотиков в отдельных странах Латинской Америки и Карибского бассейна: результаты Международного круглого стола //Наркоконтроль. – 2020. – №. 1. – С. 30–37.

9. Wang S., Zhu X. Evaluation of potential cryptocurrency development ability in terrorist financing //Policing: A Journal of Policy and Practice. – 2021. – Т. 15. – №. 4. – С. 2329-2340.

10. Naqvi S. Challenges of cryptocurrencies forensics: a case study of investigating, evidencing and prosecuting organized cybercriminals //Proceedings of the 13th International Conference on Availability, Reliability and Security. – 2018. – С. 1-5.

11. Forbes. The IRS Goes Undercover As A Bitcoin Trader In \$180,000 Sting. [Электронный ресурс]. Режим доступа URL: <https://www.forbes.com/sites/thomasbrewster/2021/09/01/irs-undercover-on-a-bitcoin-and-cryptocurrency-trading-site-in-180000-sting/>. (дата обращения: 02.04.2025).

Криставчук С. М.¹,
*курсант института подготовки
сотрудников для органов предварительного расследования
Московского университета МВД России имени В.Я.Кикотя*

Научный руководитель:
Серебрякова О. М.,
*доцент кафедры иностранных языков
Московского университета МВД России
имени В.Я. Кикотя,
кандидат филологических наук*

РАССЛЕДОВАНИЕ И СБОР ДОКАЗАТЕЛЬСТВ ПО ДЕЛАМ О КИБЕРПРЕСТУПЛЕНИЯХ

Поскольку компьютерные преступления становятся все более распространенными, это бросает серьезный вызов киберполиции во многих странах мира. Согласно разбору различных крупных дел о киберпреступлениях, можно сделать вывод, что все большее внимание уделяется важным характеристикам киберпреступлений, таким как диверсификация преступных явлений, сокрытие преступных процессов, модернизация преступных методов, а также разведданные о преступных организациях, инновации в криминальных структурах, неограниченном количестве преступных группировок и регионов, серьезных последствиях преступлений и трудностях в расследовании и сборе доказательств. Все это существенно отличает дела о киберпреступлениях от традиционных уголовных дел с точки зрения поиска улик, подачи документов на расследование, идентификации и защиты сайтов, сбора и фиксации улик, анализа доказательств и судебной идентификации, судебных разбирательств и т. д. Как мы можем выбрать соответствующую стратегию и метод расследования после возбуждения дела? Есть ли какая-либо информация, используемая в компьютерной системе? Можно ли эффективно зафиксировать и полностью извлечь эту информацию? Удастся ли успешно раскрыть дело, связанное с киберпреступностью? Нет сомнений в том, что расследование киберпреступности станет прорывом в решении всех этих проблем.

Особенности киберпреступности делают дела о киберпреступлениях явно отличными от традиционных уголовных дел с точки зрения правоохранительной базы, обнаружения улик, проведения расследования, определения на месте и защита, сбор и фиксация доказательств, судебная идентификация, а также судебные процедуры. Технология обнаружения сетей является передовой и совершенно новой профессиональной технологией в Китае и даже во всем мире [4]. Она предъявляет высокие требования к профессиональным знаниям, практическому опыту и всестороннему качеству работы следователей. Следователи нуждаются в прочном фундаменте компьютерных наук и технологий, следят за раз-

¹ © Криставчук С. М., 2025.

витием сетевых технологий, своевременно обновляют и совершенствуют структуру знаний, а также должны неоднократно участвовать в расследованиях и практике, постоянно обогащать реальный боевой опыт и повышать уровень техники и тактики. Расследование киберпреступлений, в частности, относится к органам общественной безопасности, судебной системы, госбезопасности и другим административным учреждениям, которые уполномочили органы уголовного розыска и правоохранительные органы проводить санкционированные уголовные расследования киберпреступлений на протяжении всего процесса регистрации, взлома и продажи дел, включая проверку улик.

Для эффективного предотвращения киберпреступлений и борьбы с ними при проведении расследования необходимо соблюдать три основных требования.

Требования к организации самого следственного органа. Поскольку киберпреступность является высокоинтеллектуальным и высокотехнологичным преступлением, следственным органам всех уровней необходимо располагать высокотехнологичными методами обнаружения, соответствующими таким высокоинтеллектуальным преступлениям, для выявления таких правонарушений и постоянного повышения квалификации. Кроме того, следственным органам необходимо не только постоянно обновлять собственное следственное оборудование, чтобы адаптировать его к требованиям технического расследования, но и повышать уровень профессионализма следователей.

Режим расследования – это идея или процедура, на которой основывается субъект расследования при раскрытии дела. Поскольку киберпреступность отличается от традиционной преступности, способ обнаружения киберпреступности также сильно отличается от традиционного способа расследования. Поэтому нам необходимо изучить и обобщить методы расследования киберпреступлений. Создать новый тип расследования, который является криминальным и может эффективно выявлять киберпреступления [1].

Следственные действия относятся к конкретным средствам расследования. Поскольку киберпреступность трудно обнаружить, трудно получить доказательства и трудно арестовать преступника, процент обвинительных приговоров по делам о киберпреступности крайне низок. Таким образом, в сочетании с характеристиками и законами случаев киберпреступности, обобщением и совершенствованием методов расследования это является ключом к выявлению таких преступлений.

Методы выявления случаев киберпреступлений:

1. Защита на месте киберпреступления.

Качество охраны места преступления окажет существенное влияние на то, удастся ли собрать доказательства по уголовному делу, будет ли установлен факт преступления и будет ли оно раскрыто вовремя. Киберпреступность занимает больше времени, чем традиционные преступления. Иногда это может быть не связано с географическими ограничениями, и даже может быть совершено за границей, трудно определить само место действия. Более того, поскольку объектом преступления являются неосязаемые электронные данные, компьютерная си-

стема, особенно сетевая, имеет сложную структуру, а судебно-медицинская экспертиза является технически сложной, и непреднамеренное срабатывание может привести к уничтожению улик.

Помимо случаев взлома, большинство убийств совершают киберпреступники из числа внутреннего персонала (иногда даже те, кто помогает в расследовании). Таким образом, можно проводить расследования, опираясь на данные компьютерных операторов и связанного с ними бизнес-персонала в подразделениях, занимающихся расследованием. Затем человек отправляется на место происшествия, чтобы определить место преступления [5].

2. Расследование на месте киберпреступления.

Расследование места совершения киберпреступления – это деятельность, при которой судебный орган наблюдает, осматривает место преступления в соответствии с законом, чтобы понять обстоятельства дела и собрать соответствующие доказательства. Общие методы осмотра мест совершения киберпреступлений:

- изучить дело, понаблюдать и проинспектировать площадку и определить место и объем осмотра;
- определить последовательность осмотра в соответствии с условиями на объекте и обстоятельствами дела.

Как правило, компьютер используется в качестве центра для осмотра периферии. Для более крупных сайтов можно одновременно использовать методы фрагментации, сегментации, стратификации и разделения на разделы.

3. Онлайн-отслеживание киберпреступлений.

Расследование преступной деятельности в Интернете обычно осуществляется с помощью IP-адресов доступа в Интернет, учетных записей доступа в Интернет и доступа к Интернету. В случае сетевых вторжений, если установлена надежная система обнаружения (IDS), очень полезно предотвращать и отслеживать их независимо от того, устанавливает ли пользователь систему Unix или Windows [3].

4. Отслеживание следов злоумышленников.

Вот несколько способов напасть на след потенциальных злоумышленников:

- злоумышленник будет предпринимать неоднократные попытки. Сначала злоумышленнику необходимо собрать информацию о сервере, чтобы выявить детали, которые могут быть использованы, а затем постепенно осуществлять глубокие вторжения. К примеру, в первый раз, когда сетевой администратор просмотрел журнал IDS, он обнаружил, что хакер сканирует почтовый сервер и ищет открытый порт FCD и UDP. Во-вторых, снова появился IP-адрес злоумышленника, но на этот раз его цель сосредоточилась на открытом порту; в третий раз, возможно, еще через несколько часов злоумышленник введет последовательность SMTP-команд через порт;
- схема доступа злоумышленника может дать очень важные сведения, такие как географическое местоположение, род занятий и возраст. Большинство хакеров, как правило, работают между 9 часами вечера и 3 часами ночи, и если взлом происходит только между 9 часами утра и 5 часами вечера в будние дни, то хакер может подвергнуться нападению на своем рабочем месте. Этапы процесса проникновения могут отражать уровень квалификации злоумышленника. Опытный

злоумышленник не тратит время на грамматические ошибки и повторные попытки; хакеры, пытающиеся ввести SMTP-команды через порт NNTP сетевого протокола передачи новостей, обычно являются новичками. Если вовремя проверить системный журнал после вторжения, вы можете обнаружить, что файл журнала команд в корневом каталоге учетной записи исчез. Эти признаки указывают на то, что это квалифицированная хакерская атака. Он тщательно удалил записи обо всех действиях и даже обманул сигнализацию IDS. Это похоже на то, как шпион крадет секреты, а затем стирает отпечатки пальцев. Один из способов предотвратить это – сохранить файлы журналов в нескольких местах, предпочтительно на съемном носителе, таком как дискета; вы также должны создавать резервные копии файлов журналов при резервном копировании системных данных;

– эффективно использовать IDS. Стремительный рост интернет-технологий привел к появлению новых методов атаки, и разработчикам IDS остается только обновлять свои продукты с учетом этих изменений. Другими словами, контент, который IDS может проверять и записывать, основан на методах, полученных в результате прошлых вторжений, но новые методы сетевых атак трудно обнаружить. Кроме того, даже самые сложные инструменты зондирования не могут заменить ручной анализ событий вторжения, поскольку автоматизированные инструменты не способны синтезировать информацию из разрозненных событий. Таким образом, для сетевых администраторов основная задача внедрения IDS заключается в том, чтобы отфильтровать ненужную информацию и сконцентрироваться.

Дела о киберпреступлениях характеризуются строгой секретностью и виртуальной реальностью. В дополнение к методам расследования традиционных преступлений расследование должно также изменить идеи данного процесса, изучить новые методы и принять новые меры. Многомерная криминалистическая модель (MDFM) отражает углубление криминалистического процесса с течением времени [2]. В любой момент цифровая криминалистика может быть возвращена к состоянию любого узла в соответствии с реальным процессом. Объектно-ориентированная концепция предполагает, что процессу криминалистики необходимо выбрать стратегию и определить базу знаний в соответствии с потребностями криминалистики; в редких случаях судебно-медицинский процесс делится на уровень наблюдения за доказательствами, уровень сбора доказательств и базовые данные. Три уровня, в которых данные и база знаний находятся в изначальном положении, сбор доказательств является основной работой, а механизм надзора работает на самом высоком уровне, таким образом, обеспечивается целостность цепочки доказательств и значительно повышается надежность и легитимность цифровых доказательств.

Список литературы

1. Miralis N. G., Miralis D. The 5 key challenges for law enforcement in fighting cybercrime/Miralis, N. G., Miralis, D. SEEU Review Volume? 2020.

2. Naïma Daoudi, *Electronic Crime (Characteristics, Areas of Use, and Main Methods of Combat)*/ Naïma Daoudi- Mahd Al-Lugat Review, 2020.
3. Staf T. N., *Cyberbullying: A Deadly Trend* / Staf, T. N.- Rosen Publishing, 2019.
4. Statistical report on the development of Internet in China (the 40th) August. Beijing: China Internet network information center (CNNIC), 2017.
5. Steinmetz K. F., Yar M. *Cybercrime and Society*/ Steinmetz, K. F., Yar, M., Third Edition Sage Publications, 2019.

*Мжельская Г. М.¹,
старший преподаватель кафедры иностранных языков,
Московского университета МВД России имени В.Я. Кикотя*

*Кунгурцев Т. Е.²,
курсант факультета судебной экспертизы
Московского университета МВД России имени В.Я. Кикотя*

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В США

Преступления в сфере информационных телекоммуникационных технологий на данном этапе развития общества является очень важной проблемой, которая распространена в каждой стране по-своему. Об этом виде преступлений часто можно услышать из средств массовой информации. Правонарушения, совершаемые в сфере информационных технологий, зачастую носят транснациональный характер, поскольку преступные действия могут исходить из одной страны, а их жертвами становятся граждане другой. В связи с этим для эффективной борьбы с данной категорией преступных деяний приобретает первостепенную важность международное взаимодействие и координация усилий правоохранительных органов разных государств. Конвенция Совета Европы (ETS № 185) подразделяет данные преступления на четыре группы:

- преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;
 - преступления, связанные с использованием компьютеров;
 - преступления, связанные с контентом;
 - преступления, связанные с нарушением авторских и смежных прав
- [1, ETS 185 – Convention on Cybercrime, 23.XI.2001].

Правоохранительные органы Соединенных Штатов Америки систематически взаимодействуют с многочисленным количеством государств-партнеров в сфере задержания и выдачи преступников для их последующего судебного преследования как на территории США, так и в других странах. Атаки программ-вымогателей приводят к целому ряду издержек для бизнеса. В 2023 г. Internet Crime Complaint Center (Центр подачи жалоб на преступления в Интернете) получила рекордное количество жалоб от американской общественности: 880 418 жалоб, с потенциальными потерями, превышающими \$12,5 млрд. Это почти на 10 % больше жалоб и на 22 % больше убытков по сравнению с 2022 г. [2, Alert Number: I-031824-PSA March 18, 2024 IC3 Annual Report and Fraud Flyer].

По данным IC3, преобладающее число зарегистрированных убытков связано с мошенническими действиями. Потерпевшие указывают на разнообразие ис-

¹ © Мжельская Г. М., 2025.

² © Кунгурцев Т. Е., 2025.

пользуемых мошенниками способов оплаты, включая наличные и почтовые переводы, банковские переводы, карты предоплаты и подарочные сертификаты, а также криптовалютные терминалы. Таким образом, можно сказать, что этот вид преступлений приносит Соединенным Штатам большие убытки, причем с каждым годом их число не становится меньше. Так какие же меры принимаются в Соединенных Штатах для решения этой проблемы? Например, в связи с публикацией Отчета о преступлениях в Интернете за 2024 г. Федеральное бюро расследований (ФБР) призывает граждан незамедлительно сообщать о любых подозрительных случаях, указывающих на противоправную деятельность в сети Интернет. Для этого следует воспользоваться специальной формой на сайте IC3. Подача заявлений о киберпреступлениях позволяет правоохранительным органам США своевременно реагировать на выявленные факты противоправной деятельности и способствует более эффективному противодействию киберпреступности в целом.

Можно отметить, что в Соединенных Штатах для минимизации риска киберпреступности гражданам рекомендуется соблюдать ряд профилактических мер. Основные рекомендации:

- повышение осведомленности;
- поддержание актуальности системы;
- использование надежного антивируса;
- осторожность при подключении к Wi-Fi;
- создание надежных паролей;
- многофакторная аутентификация;
- проверка адресов и ссылок;
- осторожность в социальных сетях;
- бдительность при финансовых операциях.

Каждый пользователь, подключенный к интернету, должен быть осведомлен о распространенных методах совершения киберпреступлений. Необходимо регулярно обновлять операционную систему и программное обеспечение для защиты от уязвимостей. Важно установить и использовать надежный антивирусный софт. При использовании общедоступных сетей Wi-Fi следует воздержаться от проведения финансовых операций или других действий, требующих конфиденциальности. Для каждой учетной записи необходимо использовать уникальный и сложный пароль, который регулярно меняется. Рекомендуется использовать фразу-пароль с заменой букв на специальные символы, дополняя ее текущим месяцем и названием сервиса. Где это возможно, следует активировать многофакторную аутентификацию для дополнительной защиты учетной записи. Перед открытием электронных писем или посещением веб-сайтов необходимо проверять адрес электронной почты отправителя и URL-адрес сайта. Необходимо избегать нажатия на подозрительные ссылки в нежелательных сообщениях. Не следует публиковать личную информацию, которая может быть использована злоумышленниками для взлома учетных записей (имена домашних животных, членов семьи, названия учебных заведений). Необходимо быть осторожным при отправке

платежей неизвестным лицам или организациям, особенно если они требуют немедленных действий и создают атмосферу паники.

В Соединенных Штатах Америки активно внедряется модель межведомственного взаимодействия в сфере противодействия киберпреступности. Для реализации этой модели создаются специализированные центры, объединяющие усилия представителей государственных органов, частного сектора и научного сообщества. Целью таких центров является построение прочных и доверительных отношений между участниками, что позволяет эффективно выявлять и пресекать киберугрозы. Ярким примером такого центра является Национальная совместная группа по расследованию киберугроз (NCIJTF). Национальный центр по борьбе с киберпреступностью (NCIJTF), будучи уникальным межведомственным центром, играет ключевую роль в координации, интеграции и обмене информацией. Его миссия заключается в поддержке расследований киберугроз, предоставлении и анализе разведывательных данных для лиц, принимающих решения на государственном уровне, а также в усилении эффективности существующих мер по борьбе с киберугрозами в стране.

Также хочется отметить Агентство по кибербезопасности и безопасности инфраструктуры (CISA) оно работает с партнерами для защиты от современных угроз и сотрудничает с промышленностью для создания более безопасной и устойчивой инфраструктуры в будущем. CISA находится в центре мобилизации коллективной обороны, чтобы управлять и понимать риски критически важной инфраструктуры. Партнерами в этой миссии являются государственный и частный секторы. Предоставляемые программы и услуги основаны на всестороннем понимании среды рисков и соответствующих потребностей, определенных заинтересованными сторонами. CISA стремится помочь организациям лучше управлять рисками и повышать устойчивость, используя все доступные ресурсы, будь то федеральное правительство, коммерческие поставщики или их собственные возможности [3, CISA Fact Sheet Revision Date October 25, 202]. Таким образом изучив подробнее CISA можно выявить их основную деятельность в борьбе с киберпреступностью: CISA предоставляет услуги и техническую поддержку, инструменты и учения, учебные программы и мероприятия по повышению осведомленности граждан, что способствует улучшению понимания общих рисков и возможных стратегий их минимизации. Эта организация является федеральным лидером в области реагирования на киберинциденты, работая совместно с частным сектором и правительствами штатов, местными и территориальными органами власти, а также федеральными агентствами. Кроме того, CISA координирует свои действия с партнерами из государственного и частного секторов для обеспечения поддержки специальных мероприятий по национальной безопасности, таких как Суперкубок. Агентство предлагает стратегии управления рисками, помогая заинтересованным сторонам управлять последствиями возникающих и будущих рисков. CISA собирает и анализирует данные для информирования и приоритизации мер по управлению рисками, что позволяет определить критически важные инфраструктуры и связанные с ней национально-критические функций. CISA использует инструменты и технологии для оценки кибер- и физических угроз для людей и имущества, а также потенциальных последствий этих

опасностей. CISA способствует улучшению коммуникации в области общественной безопасности на всех уровнях государственного управления.

Существует еще Отдел по борьбе с компьютерными преступлениями и интеллектуальной собственностью (CCIPS), который является одним из подразделений Министерства Юстиции Соединенных Штатов. В его компетенции входит расследование компьютерных преступлений и преступлений в сфере интеллектуальной собственности.

К сожалению, не существует, как такового, подхода для полного пресечения этого вида преступления. Неутешительная статистика говорит о том, что киберпреступлений совершается все больше и больше. В современном мире невозможно полностью пресечь эти преступления, можно лишь уменьшить их количество за счет повышения осведомленности населения и создания специальных отделов по борьбе с компьютерными преступлениями.

Список литературы

1. ETS 185 – Convention on Cybercrime, 23.XI.2001 <https://base.garant.ru/4089723/?ysclid=m9isrwi2f4246786789>.
2. Alert Number: I-031824-PSA March 18, 2024 IC3 Annual Report and Fraud Flyer.
3. CISA Fact Sheet Revision Date October 25, 2021.

Соломина А. А.¹,

*курсант 2 курса института подготовки сотрудников
для органов предварительного расследования*

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Старова Е. В.,

преподаватель кафедры иностранных языков

Московского университета МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ (ГИС) И КРИМИНАЛЬНОЙ АНАЛИТИКИ КАК МЕТОДА ПРОГНОЗИРОВАНИЯ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ

Современные карты криминогенности, аккумулирующие статистику по преступлениям, уже давно существуют во многих странах, в том числе со статистикой по отдельным городам. Однако в большинстве случаев эти данные отражают ретроспективную картину без привязки к уникальным особенностям конкретного муниципалитета. Для профилактики преступлений эта информация должна быть интегрирована с геоинформационными сервисами (ГИС) каждого региона. Например, маркировка потенциальноопасных объектов (заброшенные здания, гаражные комплексы, пустыри, лесопарковые зоны), а также мест скопления людей (образовательные учреждения, торгово-развлекательные центры и пр.) позволит выявить возможные локации преступлений. Эта идея легла в основу национальной карты опасных мест, где ребенок может попасть в беду во время летних каникул. Это предложение впервые прозвучало на всероссийском совещании детских омбудсменов в Ярославле в 2017 году.

ГИС-технологии (географическая информационная система) – это цифровой инструмент для работы с пространственными данными. В своей деятельности правоохранительные органы как в России, так и за рубежом пользуются определенными алгоритмами для решения задач разной сложности. Например, сотрудники правоохранительных структур анализируют закономерности региональной преступности и на федеральном уровне, относительно определенного этноса или гражданства (подданства); выявляя горячие точки криминальной активности, а также учитывают связь преступлений в соответствии с городской инфраструктурой, временем года, суток и днями недели.

Таким образом, данные ГИС технологии помогают прогнозировать всплески криминальной активности в определенном районе. Кроме того, у ГИС технологий есть еще одна прикладная функция, которая заключается в визуализации, т. е. в создании интерактивных карт, отслеживании перемещений подозреваемых и обвиняемых лиц и др.

¹ © Соломина А. А., 2025.

Например, геоинформационная система может показать, что в определенном районе каждую пятницу вечером увеличивается число краж, и предложить усилить там патрулирование. Анализ данных за последние пять лет в Москве показал, что около 65 % уличных краж совершается в радиусе 500 метров от станций метро в вечернее время.

Основные методы пространственного анализа включают в себя анализ горячих точек, визуализацию, ядерную оценку плотности распределения. Метод анализа горячих точек – это выявление зон с аномально высокой концентрацией преступлений. Например, в США используется алгоритм PredPol, который на основе исторических данных выделяет квадраты на территории штатов (500×500 м), где вероятность преступлений наиболее высока. Вследствие чего наблюдается снижение краж на 12–25 % в тестовых районах. Отечественный опыт показывает, что использование технологии системы «Безопасный город» выявляет неблагоприятные зоны совершения правонарушений в определенных локациях, что дает возможность распределять правоохранительные силы соразмерно полученному анализу, усиливая зоны потенциальной активности преступной деятельности.

Метод ядерной оценки плотности распределения заключается в создании «тепловой карты» местности для визуализации зон наибольшего риска. В Бразилии благодаря данному алгоритму сотрудники органов внутренних дел анализируют убийства с помощью данного метода. Выявлено, что 70 % преступлений сосредоточены в так называемых фавелах (кварталы в бразильских мегаполисах с плотной спонтанной застройкой, их также называют трущобами.) В России в Казани, по данным ГИС МВД России, наибольшая плотность грабежей наблюдалась в центре города и районе «Горки», и, как результат, были установлены дополнительные камеры видеонаблюдения.

Пространственно-временной анализ позволяет выявить закономерности не только в пространстве, но и во времени (например, сезонность преступлений). В Чикаго при анализе перестрелок система HunchLab выявила, что чаще всего стрельбы происходят по пятницам вечером в районах, где проживает население с низким уровнем дохода. В России в Краснодарском крае был выявлен пик краж в летние месяцы в парках и у торговых центров.

Опыт показывает, там, где внедряют ГИС-аналитику, уровень преступности снижается на 10–30 %. В России такие системы помогают быстрее раскрывать преступления и эффективнее распределять патрули, что уменьшает уровень уличной преступности на 15–20 %. В соответствии со статистическими данными в США (PredPol), Великобритании (RIOT) и Китае (Skynet) ГИС-аналитика снизила уровень преступности на 10–30 %.

Особую ценность представляет интеграция ГИС с другими цифровыми технологиями. Совмещение картографических данных с информацией из систем видеонаблюдения, данных сотовых операторов и социальных медиа создает комплексную картину криминогенной обстановки. В Китае система Skynet, объединяющая более 200 миллионов камер с технологией распознавания лиц, помогла значительно повысить раскрываемость преступлений.

Однако внедрение ГИС-технологий сталкивается с определенным рядом вызовов. Основные проблемы включают неполноту и разрозненность данных

между различными ведомствами, необходимость защиты персональных данных, а также риск алгоритмических ошибок. Так, в некоторых американских городах были зафиксированы случаи, когда системы прогнозирования преступлений демонстрировали расовую предвзятость.

Перспективы развития ГИС в криминальной аналитике связаны с внедрением технологий искусственного интеллекта, обработки естественного языка и компьютерного зрения. Особое значение приобретает создание межведомственных платформ, позволяющих объединять данные из различных источников. В России этот процесс идет в рамках программы «Умный город» и проекта «Безопасный регион». Для отечественного опыта применения ГИС-технологий можно выделить следующие рекомендации: обратить внимание на опыт ЕС и иных государств по этичному ИИ (исследование влияния этнических и культурных особенностей на восприятие и использование искусственного интеллекта). Также необходимо практиковать взаимодействие между различными организациями и ведомств с МВД России (Американские практики публично-частного партнерства (университеты + полиция), например, интеграция МВД России, Росгвардии, муниципалитетов).

Список литературы

1. Алпеева О. И., Бушуева А. В. Применение цифровых технологий и искусственного разума при предупреждении преступности // Вестник ПензГУ. 2021. № 3 (35). – 54–62 с. URL: <https://cyberleninka.ru/article/n/primenenie-tsifrovyyh-tehnologiy-i-iskusstvennogo-razuma-pri-preduprezhdenii-prestupnosti> (дата обращения: 13.04.2025).
2. Альховская А. В., Худяков В. В., Воробьева Т. И. Применение геоинформационных технологий в профессиональной деятельности сотрудников полиции // Международный журнал гуманитарных и естественных наук. 2022. № 3-1. С. 88. URL: <https://cyberleninka.ru/article/n/primenenie-geoinformatsionnyh-tehnologiy-v-professionalnoy-deyatelnosti-sotrudnikov-politsii> (дата обращения: 13.04.2025).
3. Вичугова А. А. Как сделать город безопасным: Big Data и Machine Learning против преступности, 2020. URL: <https://bigdataschool.ru/blog/crime-mapping.html>.
4. Труханова Э. И. В России появится интерактивная карта опасных мест для детей, 2019. URL: https://rg.ru/2019/07/11/reg-cfo/v-rossii-poiavitsia-interaktivnaia-karta-opasnyh-mest-dlia-detej.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F.
5. Отчет МВД РФ «О практике применения ГИС-технологий» URL: <https://77.мвд.рф/гу-мвд/структура-управления/управления/правовое-управление/результаты-работы/за-2023-год>.

Хмирова Е. А.¹,

старший преподаватель кафедры иностранных языков

Московского университета МВД России имени В.Я. Кикотя

Кузнецова С. А.²,

курсант 531 учебного взвода 2 курса

международно-правового факультета

Московского университета МВД России имени В.Я. Кикотя

ОПЫТ КИТАЯ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Проблема кибербезопасности приобретает все большую актуальность для государственных органов и бизнеса по всему миру.

Китай появился на арене кибербезопасности сравнительно недавно. Бурный рост сети Интернет за последние двадцать лет привел к радикальным изменениям в жизни китайского общества. Однако Интернет также породил серьезные вызовы для Китая, затрагивающие политическую, экономическую, военную и социальную сферы, а также права и законные интересы граждан.

В ноябре 2016 г. Китай для укрепления кибербезопасности принял Закон Китайской Народной Республики о кибербезопасности.

Этот закон стал главным звеном формирующейся стратегии Китая в области киберпространства. При его разработке Китай частично опирался на законодательный опыт США, Великобритании и других стран, сохраняя при этом собственные национальные особенности.

Китай построил свое первое подключение к Интернету в 1994 г. и с тех пор стал одним из крупнейших интернет-рынков в мире. Сегодня в Китае больше всего пользователей Интернета в мире – 710 миллионов, по сравнению с 460 миллионами в Индии и 290 миллионами в Соединенных Штатах. Пользуясь удобством поисковых систем, социальные сети, большие данные и облачные вычисления, пользователи Интернета также подвержены различным киберугрозам, таким как хакерские атаки, слежка и утечка личной информации. Китай является одной из стран, которые страдают от наиболее серьезных угроз со стороны интернета. Большинство этих угроз исходит из Китая, общее число случаев составило 126 424 и рост в годовом исчислении составил 128, 6%. Некоторые из этих инцидентов вызвали значительный социальный резонанс. Например, в 2013 г. произошла утечка и продажа личной информации более миллиона клиентов УТО Express, крупной курьерской службы в Китае. В 2014 г. ведущая китайская компания Агентство по онлайн-бронированию путешествий Strip.com сообщило, что оно обнаружило и устранило лазейку в безопасности, которая делала информацию о кредитных картах пользователей уязвимой для взлома. Всплеск этих тревожных инцидентов в области кибербезопасности не только пробудил в людях осведомленность о кибербезопасности, но и укрепил решимость китайского пра-

¹ © Хмирова Е. А., 2025.

² © Кузнецова С. А., 2025.

ительства улучшить управление киберпространством. С точки зрения китайского правительства, для обеспечения кибербезопасности необходим всеобъемлющий закон о киберугрозах. В частности, с тех пор, как Си Цзиньпин стал президентом, он неоднократно подчеркивал важность продвижения законов о кибербезопасности, включая Всемирную конференцию по Интернету и заседания Центральной руководящей группы по киберпространствам.

Статья 1 Закона о кибербезопасности определяет его главную цель: обеспечение кибербезопасности, защиту суверенитета в киберпространстве, национальной безопасности, общественных интересов, а также законных прав граждан, организаций и предприятий. Закон также направлен на стимулирование здорового развития информатизации экономики и общества.

Данный закон основывается на принципе национальной безопасности, провозглашенном в Законе о национальной безопасности Китая, и ставит суверенитет в киберпространстве на первое место. Для достижения этой цели закон акцентирует внимание на защите безопасности сетевых операций, критической информационной инфраструктуры и онлайн-информации.

В то же время китайское правительство активно участвует в международном сотрудничестве в сфере кибербезопасности, способствуя развитию интернет-экономики при одновременном сохранении национального суверенитета в киберпространстве.

Закон о кибербезопасности устанавливает нормы поведения для государственных органов, коммерческих организаций и граждан в отношении доступа к Интернету. Общие положения закона определяют его сферу действия, национальную политику в области кибербезопасности, правоприменительные органы, основные принципы и специальные меры защиты несовершеннолетних пользователей. Как первый базовый закон Китая, регулирующий кибербезопасность, «Закон о кибербезопасности» включает в себя несколько важных принципов и новшеств, таких как суверенитет в киберпространстве, иерархическая система защиты кибербезопасности, система защиты критически важной информационной инфраструктуры, система оценки безопасности для трансграничной передачи данных и система оценки безопасности сетевых продуктов и услуг.

В официальном документе, опубликованном китайским правительством в июне 2010 г., Интернет объявлен критически важным элементом государственной инфраструктуры. В нем подчеркивается необходимость подчинения китайской сети национальной юрисдикции и уважения суверенитета Китая в киберпространстве. На Первой всемирной конференции по интернету в ноябре 2014 г. президент Си Цзиньпин выступил с речью, в которой заявил о готовности Китая к сотрудничеству с другими странами для укрепления международного взаимодействия, уважения суверенитета Интернета и обеспечения кибербезопасности. Данное заявление стало первым официальным предложением концепции суверенитета в киберпространстве со стороны китайского правительства. Суверенитет в киберпространстве рассматривается как естественное продолжение национального суверенитета и подразумевает соблюдение основных принципов, таких как равноправие государств, мирное разрешение споров и уважение к внутренним делам других стран. Данная концепция включает в себя четыре основных права:

1. Право юрисдикции – право страны управлять сетями на своей территории.
2. Право на самооборону.
3. Право на независимость.
4. Право на равенство.

Согласно Закону о кибербезопасности, статья 2 которого предусматривает действие закона на всей территории Китайской Народной Республики в отношении создания, эксплуатации, обслуживания и использования сетей, а также надзора и управления кибербезопасностью, китайское правительство осуществляет территориальную юрисдикцию во всех вопросах, связанных с сетями в Китае. Это положение распространяется на все субъекты, связанные с Интернетом на территории Китая (включая интернет-провайдеров, операторов сетей, пользователей Интернета, регулирующие органы и т. д.), а также на материалы, сетевую информацию и саму кибердеятельность. Таким образом, любая кибердеятельность, осуществляемая на территории материкового Китая, подлежит действию китайского законодательства независимо от национальной принадлежности участников. Право на самооборону относится к праву суверенного государства на защиту от кибератак и угроз извне. Статья 5 Закона о кибербезопасности гласит, что «государство принимает меры по мониторингу, предотвращению и устранению рисков и угроз кибербезопасности, возникающих как на материковой территории Китая, так и за ее пределами. Государство защищает критически важную информационную инфраструктуру от атак, вторжений, вмешательства и разрушения. Государство наказывает за незаконную и преступную кибердеятельность в соответствии с законом, сохраняя безопасность и порядок в киберпространстве. Это положение подтверждает право Китая на оборону в киберпространстве и позволяет китайскому правительству отслеживать, защищаться и наказывать иностранные кибератаки и угрозы.

Статья 75 Закона о кибербезопасности КНР предусматривает применение мер по замораживанию активов или иных санкций в отношении организаций и физических лиц, чьи действия направлены на создание угрозы критически важной информационной инфраструктуре КНР, если такие действия приводят к серьезным последствиям. Это положение законодательства реализует право на самооборону, закрепленное в статье 5, и устанавливает правовую базу для пресечения зарубежных кибератак и слежки. В документе также подчеркивается принцип суверенитета в киберпространстве, который означает право страны самостоятельно определять свою политику в сфере кибербезопасности, разрабатывать соответствующие законы и нормативные акты, защищать свои информационные системы и ресурсы от внешних угроз, а также сохранение законных прав и интересов своих граждан в киберпространстве. При этом страны должны уважать суверенитет друг друга в киберпространстве и воздерживаться от вмешательства во внутренние дела других государств. Статья 7 Закона о кибербезопасности призывает к созданию мирного, безопасного, открытого и совместного киберпространства, а также к формированию многосторонней, демократической и прозрачной системы управления Интернетом, что отражает принцип равенства в доступе ко всемирной сети. В своей стратегии международного сотрудничества в сфере киберпространства Китай придерживается принципа равноправия всех государств.

Независимо от их размера, экономической мощи или политического влияния все страны имеют право на равное участие в формировании международных норм и правил в киберпространстве. Китай подчеркивает необходимость использования международных механизмов и платформ для обеспечения того, чтобы будущее киберпространства было определено всеми народами. Закон о кибербезопасности Китая расширяет понятие «операторы сетей», включая не только традиционных провайдеров связи, но также организации и частные лица, предоставляющие услуги через интернет. Это означает, что все субъекты, участвующие в функционировании онлайн-пространства, от владельцев веб-сайтов до поставщиков информационных услуг, несут ответственность за соблюдение законодательных требований.

Закон обязывает операторов сетей, независимо от источника финансирования, выполнять свои юридические обязательства, связанные с обеспечением кибербезопасности. Они должны соответствовать государственным стандартам и принимать необходимые технические меры для предотвращения киберпреступлений, обеспечения целостности данных и стабильности работы сетей.

Обязательства поставщиков сетевых продуктов и услуг в соответствии с Законом о кибербезопасности КНР. Согласно статье 22 Закона о кибербезопасности Китайской Народной Республики, поставщики сетевых продуктов и услуг обязаны соблюдать следующие требования:

1. Соответствие стандартам: продукция и услуги должны соответствовать установленным национальным стандартам.
2. Отсутствие вредоносных программ: поставщики не вправе внедрять вредоносные программы в свои продукты и услуги.
3. Немедленное устранение уязвимостей: в случае обнаружения недостатков безопасности или уязвимостей, поставщики обязаны незамедлительно принять меры по их исправлению, проинформировать пользователей и компетентные органы.
4. Постоянное обеспечение безопасности: поставщики должны обеспечивать непрерывную защиту своих продуктов и услуг в течение срока, установленного законодательством или согласованного сторонами.

Эти требования являются минимальными для всех поставщиков сетевых продуктов и услуг. В дополнение к общим обязательствам, Закон о кибербезопасности предусматривает систему тестирования и сертификации для критически важного сетевого оборудования и продуктов кибербезопасности (Статья 23). Такие продукты должны соответствовать национальным стандартам и обязательным требованиям, а также проходить проверку и сертификацию в квалифицированном учреждении до начала продажи или предоставления. В ответ на замечания международных организаций о потенциальном увеличении затрат и торговых барьеров, китайское правительство планирует создать каталог критически важного сетевого оборудования и продуктов кибербезопасности, а также способствовать взаимному признанию результатов проверок и сертификации.

Первый выпуск каталога уже опубликован и включает в себя ключевое оборудование, такое как маршрутизаторы, серверы, системы защиты от спама и другие специализированные продукты. Учитывая важность и сложность проверки

безопасности сети, правительство Китая также опубликовало Временные меры по проверке безопасности для сетевых продуктов и услуг для реализации положений Закона о кибербезопасности.

Более десяти лет назад Китай начал внедрять систему сетевых реальных имен. Изначально, в 2003 г., местные органы власти, контролирующие интернет-кафе, обязали пользователей предоставлять удостоверения личности для регистрации под своим настоящим именем. В 2004 г. Министерство образования выпустило документ, призывающий к внедрению системы «реальных имен» в университетских сетях. К 2005 г. ряд ведущих университетов перешел на внутренние коммуникационные платформы, основанные на системе реальных имен. В последующие годы местные власти, такие как Ханчжоу и Пекин, также приняли соответствующие правила и положения. В 2012 г. Постоянный комитет принял решение об усилении защиты онлайн-информации, которое обязывает поставщиков сетевых услуг получать реальную идентификационную информацию от клиентов при предоставлении доступа в Интернет, стационарной и мобильной связи, а также услуг по распространению информации. В 2015 г. Государственное информационное управление Интернета опубликовало Положения об управлении именами пользователей Интернета, а в 2016 г. Административный регламент о мобильных интернет-информационных услугах также предусматривает необходимость получения реальной информации о клиентах от провайдеров мобильных интернет-приложений.

Китайский Закон о кибербезопасности (2016) отражает стратегический подход страны к защите национального суверенитета и безопасности в цифровом пространстве. Акцент на регулировании критической инфраструктуры, контроль данных и сотрудничество с международными партнерами демонстрируют стремление балансировать между безопасностью и развитием. Однако закон также вызывает вопросы о соотношении контроля и свобод, характерных для китайской модели управления интернетом. В будущем его реализация потребует адаптации к новым технологическим вызовам и глобальным стандартам.

Список литературы

1. «О кибербезопасности»: закон Китайской Народной Республики от 1 июня 2017 г. // Официальный сайт Постоянного комитета ВСНП.
2. Cheung, T. M. «China's Cybersecurity and Information Warfare» / T. M. Cheung. – Santa Barbara : Praeger, 2021. – 280 p. – ISBN 978-1-4408-7535-8.
3. Creemers, R. Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century / R. Creemers // «Journal of Contemporary China». – 2017. – Vol. 26, № 103. – P. 85–100.
2. Zeng, J., Stevens, T. China's Smart State Surveillance: AI and the Reshaping of Cyber Sovereignty / J. Zeng, T. Stevens // «Survival». – 2021. – Vol. 63, № 2. – P. 7–32.

Яценко С. И.¹,

курсант 2 курса института

подготовки сотрудников для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Старова Е. В.,

преподаватель кафедры иностранных языков

Московского университета МВД России имени В.Я. Кикотя

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В ВЕЛИКОБРИТАНИИ

Цифровые технологии стали неотъемлемой частью повседневной жизни человеческого общества. Цифровизация незаметно вошла во все сферы жизни человека.

Великобритания является одной из самых зависимых в цифровом отношении экономик мира и, как следствие, пропорционально увеличивается рост киберпреступлений. В Великобритании любая незаконная деятельность с использованием информационных технологий подпадает под категорию киберпреступлений.

К такого вида преступлениям относятся: кибермошенничество, финансовые преступления, кража информации кредитных карт населения, взлом банковских счетов, онлайн-мошенничество; нарушение авторских прав «пиратство» (загружая и распространяя нелегальные копии программного обеспечения, музыки, фильмов или других материалов, защищенных авторским правом); кибератаки и терроризм, включая взлом компьютерных систем государственных учреждений, критически важных объектов инфраструктуры и частных компаний с целью нанесения ущерба, вызывая сбои в работе; кибербуллинг и онлайн-домогательства (используя интернет и социальные сети для угроз, запугивания и оскорблений); нарушения конфиденциальности и утечка личной информации (получая незаконный доступ к информации личных данных, частной жизни, медицинской и финансовой информации человека).

Наказания за совершение киберпреступлений варьируются от штрафов до тюремного заключения на различные сроки. Данного вида преступления в Великобритании рассматриваются уголовным законодательством как мошенничество, включая 14 категорий.

В 2016 г. в Великобритании был основан Национальный центр компьютерной безопасности (НЦБК) для обеспечения защиты от хакерских атак и своевременного выявления угроз оперативного реагирования на совершаемые преступления.

Приоритетной задачей политики и развития государства становится защита общества и населения от киберпреступлений, так как ущерб, причиняемый такими преступлениями в социальной и экономической сферах страны, отражается на

¹ © Яценко С. И., 2025.

национальном благополучии страны. Государство должно обеспечить высокий уровень кибербезопасности для обеспечения защиты от сдерживания ряда угроз критически жизненно важной национальной инфраструктуры и снизить возможные риски.

Национальный центр компьютерной безопасности разработал Национальную стратегию кибербезопасности страны. В данном документе определено три организационных принципа – это защита, сдерживание и развитие. Первый принцип способствует эффективной защите от киберугроз и реагированию на них. Принцип «Сдерживание» направлен на выявление, понимание и противодействие враждебным кибероперациям, в том числе использование ответного наступательного движения в соответствие со своими кибервозможностями. Принцип «Развитие» необходим для проведения исследований и разработок современного технологического инструментария в области кибербезопасности, используя инновации, а также образовательные и обучающие программы для удовлетворения потребностей как государственного, так и частного секторов в квалифицированных кадрах.

Национальный центр компьютерной безопасности работает также над выявлением уязвимых мест в Интернет-ресурсах, устраняя возникающие угрозы. С помощью специализированной программы киберзащиты фишинговый сайт будет существовать не более 27 часов.

Основная масса кибератак осуществляется инструментами и методами, легко доступными в онлайн пространстве. Такие атаки, как правило, нацелены не на конкретные компании и частные лица, а на как можно большее количество объектов. Например, «фишинг» работает путем рассылки электронных писем как можно большему числу людей. Если даже небольшой процент тех, кто получает электронные письма, будет обманут, можно получить существенную отдачу от незначительных затрат.

Великобритания располагает широким спектром воздействия для противодействия кибератакам. Разрабатываются и применяются имеющиеся кибервозможности для проведения операций по защите киберпространства, предотвращения и раскрытия правонарушений. Операции проводятся с применением методов, позволяющих сделать технологии злоумышленников менее эффективными или полностью заблокировать их функционирование.

Кроме этого, могут использоваться различные методы для снижения способности правонарушителей распространять дезинформацию и запрещенные медиа в Интернете. Используется сочетание технических и информационных операций против правонарушителей взаимодополняющим образом, например, чтобы посеять недоверие в таких группах, как преступные банды или террористические ячейки.

В 2019 г. в Соединенном Королевстве утверждены правила, которые предписывали IT-компаниям обеспечивать информационную безопасность своих клиентов и нести ответственность в случае нанесения им вреда. Также они должны принимать исчерпывающие меры для защиты своих пользователей от киберугроз.

В 2021 г. в Великобритании была опубликована новая НСКБ, согласно которой создаются новые платформы обучения граждан навыкам информационных технологий.

Кроме этого, НЦКБ обеспечивает безопасность граждан при взаимодействии с правоохранительными органами; расширение исследовательского потенциала НЦКБ; использование безопасной продукции Интернет-ресурсов потребительских продуктов, осуществление крупных финансовых вложений в информационную безопасность государственного сектора.

Основные направления Национальной программы кибербезопасности в Великобритании в 2024 г.:

1. Оценка и управление информационными рисками. Это направление включает продукты или услуги, которые помогают организациям справляться с киберрисками, например, с соблюдением кибербезопасности или утечкой данных.

2. Безопасность интернета включает продукты или услуги по встраиванию или модернизации безопасности устройств или сетей интернета.

3. Сетевая безопасность включает аппаратное или программное обеспечение, предназначенное для защиты работоспособности и целостности сети.

4. Безопасность систем SCADA и информационного контроля включает кибербезопасности промышленных систем управления, критически важной национальной инфраструктуры и операционных технологий.

5. Мониторинг, обнаружение и анализ угроз включает мониторинг или обнаружение различных форм угроз для сетей и систем.

6. Обучение, информирование и образование включает продукты или услуги, связанные с кибербезопасностью, обучением и образованием.

В 2024 г. многие компании в Великобритании столкнулись с кибермошенничеством, половина из которых были атакованы повторно. Встречались следующие виды кибератак:

1. Фишинговые атаки (90 % от общего числа). Мошенники рассылают поддельные сообщения и призывы, которые, кажется, исходят из надежного источника. Фишинговый контент обманом заставляет людей передавать конфиденциальные данные, например, данные кредитной карты и входа в систему.

2. Взлом (10 %). Несанкционированный доступ или онлайн-захваты.

3. Вирусы, шпионское ПО или вредоносное ПО (2%). Это программное обеспечение, разработанное хакерами для кражи данных и повреждения или уничтожения компьютерных систем. Хакеры продают украденные в результате вредоносных атак данные для дальнейших криминальных схем.

4. Программы-вымогатели (2 %). Злоумышленники блокируют системы и требуют выкуп. Такие атаки представляют собой наиболее непосредственную угрозу критически важной инфраструктуре, включая энергетику, транспорт, водоснабжение, здравоохранение и телекоммуникации.

5. Атаки типа «Отказ в обслуживании» (1 %) используются хакерами для нарушения работы организаций. В результате взлома устройства заполняются разрушительными ложными запросами, мешающими людям выполнять даже простые задачи.

Мошенники активно используют генеративный искусственный интеллект и клонирование голоса. Практически 50 % компаний считают кибератаки главной проблемой в предотвращении мошенничества. В 2025 г. Великобритания сталкивается с ростом кибератак и многие из них связаны с программами-вымогателями. Кибератаки осуществляются с целью получения финансовой выгоды, краж интеллектуальной собственности, психологического воздействия, распространения дезинформации. По информации на январь 2025 г. правительство Великобритании предлагает три подхода к борьбе с кибератаками программ-вымогателей:

1. Полный запрет на выплату выкупа со стороны государственных организаций и ключевых инфраструктурных объектов. Власти считают, что такая мера сделает эти объекты менее интересными для злоумышленников.

2. Частное организациям, не входящим в государственный сектор, придется получать специальное разрешение от правительства перед выплатой выкупа. Такая «лицензия на выкуп» будет выдаваться только в очень редких случаях.

3. Обязательное уведомление о кибератаках без ограничений на совершение выкупа. Такой подход поможет правоохранителям собирать больше данных для расследований, но вряд ли снизит активность преступников.

Кроме того, каждая организация, независимо от размера, должна инвестировать в свою безопасность, использовать проверенные инструменты и регулярно тестировать планы своего восстановления после возможных атак.

Эксперты подчеркивают, что рост мошенничества, основанного на искусственном интеллекте, требует изменения подхода к безопасности платежей. В условиях растущих угроз кибермошенничества компаниям необходимо перейти к более технологически продвинутым решениям для защиты своих финансовых операций.

В ходе борьбы с киберпреступлениями большое внимание уделяется профилактике и неотвратимости наказания виновных. Однако в настоящее время цифровая экономика в Великобритании отсутствует правовое регулированное общественных отношений в сфере цифровой экономики. Кроме этого, огромную озабоченность вызывает проблема защита персональных данных граждан, их имущества и др. Эти проблемы требуют особого внимания со стороны государства для эффективного противостояния киберпреступлениям.

Список литературы

1. Национальная киберстратегия Великобритании. Национальные киберсилы // URL: <https://wikivisa.ru/blog/blogi-ekspertov/natsionalnaya-kiberstrategiya-velikobritanii-ncs-natsionalnye-kibersily-ncf-8340/>.
2. Национальная киберстратегия до 2022 года (НКБ) // URL: <https://www.gov.uk/government/publications/national-cyber-strategy-2022/>.
3. Национальная программа информационной безопасности Великобритании // URL: <https://www.tadviser.ru/index.php/>.
4. Тим Стивенс, Майкл О'Брайен, Ричард Оверилл и др. Активная киберзащита Великобритании: Общественное благо для частного сектора // URL: <https://www.kcl.ac.uk/policy-institute/assets/uk-active-cyber-defence/>.