МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛГОГРАДСКАЯ АКАДЕМИЯ

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ В РОССИИ

Сборник научных трудов

Волгоград
ВА МВД России
2025

УДК 343.13(082)
ББК 67.410.2я43
П 78

Одобрено
редакционно-издательским советом
Волгоградской академии МВД России

П 78 **Проблемы** и перспективы развития предварительного следствия в России : сборник научных трудов / редколлегия : М. А. Бугера, Ю. С. Сафонова, О. С. Шамшина [и др.]. – Электрон. дан. (0,8 Мб). – Волгоград : ВА МВД России, 2025. – 1 электрон. опт. диск (DVD-R). – Систем. требования : частота процессора не менее 2 ГГц ; операционная система от Windows XP SP3 до Windows 11 ; оперативная память не менее 2 Гб ; 0,8 Мб свобод. диск. пространства ; разрешение экрана не менее 800 х 600 ; оптический привод DVD-ROM/RW ; Adobe Acrobat Reader 8.0 и выше. – Текст : электронный.

ISBN 978-5-7899-1619-3

Сборник составлен по материалам Всероссийской научно-практической конференции «Актуальные проблемы расследования преступлений, совершенных в сфере информационно-телекоммуникационных технологий в современных условиях» и Всероссийской научно-практической конференции «Моя профессия – следователь» (посвященной 62-й годовщине образования органов предварительного следствия в системе МВД России), проведенных на базе Волгоградской академии МВД России.

Издание предназначено курсантам, слушателям, адъюнктам и педагогическим работникам образовательных организаций системы МВД России, сотрудникам органов внутренних дел Российской Федерации.

УДК 343.13(082)
ББК 67.410.2я43

ISBN 978-5-7899-1619-3

СОДЕРЖАНИЕ

РАЗДЕЛ I.
АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННЫХ УСЛОВИЯХ

(Всероссийская научно-практическая конференция,
Волгоградская академия МВД России, г. Волгоград, 26 марта 2025 г.)

Константин Михайлович Бондарь,
профессор кафедры информационного и технического
обеспечения органов внутренних дел
Дальневосточного юридического института
МВД России имени И. Ф. Шилова,
кандидат технических наук, доцент

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ В ПРОТИВОДЕЙСТВИИ IT-ПРЕСТУПЛЕНИЯМ

Совокупность современных информационных источников Интернета – социальных сетей и других – обладает несколькими характеристиками, которые привлекают все большее количество пользователей. Среди таких характеристик – общемировая доступность, простые алгоритмы интерфейсов, очень большие объемы открытой полезной, значимой разноплановой информации, возможность организовать сервисы управления различными процессами на территориях любого масштаба и т. д. [1].

Отмеченные положительные свойства определяют условия цифровизации общества, перевод его на новые уровни эффективного управления, получение перечня разнообразных услуг и многое другое. В то же время диалектическое единство процессов прогресса и регресса формирует и развивает, наряду с ожидаемыми и необходимыми достижениями, и негативные явления, в частности, относимые к кибер- (или IT-) преступности.

Перечисленные особенности мирового информационного пространства способны помочь объективно необходимому государственному противодействию указанным противоправным деяниям. Об уровне технологического обеспечения возможности оказания этой помощи свидетельствует, прежде всего, наличие информационно-аналитических систем, специализированных аппаратно-программных комплексов (АПК), которые по сути выполняемого функционала относятся к средствам открытой информационной разведки, важным для получения информации из открытых источников в Интернете. Основная задача названных систем и комплексов – анализ данных и выявление взаимосвязей между событиями. Потенциал подобных средств включает поиск профилей людей, их имен, сфер деятельности организаций, названий компаний и др. К их функциям следует отнести, например, фильтрацию фейковых новостей, осуществление поиска по фотографиям, текстам и источникам. В период военных действий (подобных тем, что осуществляются в настоящее время на территории Украины) системы и комплексы такого типа становятся ключевым инструментом, посредством которого организуется противостояние внешним угрозам. В целом же использование информационно-аналитических систем, предоставляющее доступ к данным, получаемым с помощью спутников, а также посредством при-

менения других современных технологий, специально разработанных в изучаемой сфере, призвано способствовать раскрытию преступлений, определению местоположения агрессоров, IT-преступников, фиксированию их действий.

Вначале отметим негативные моменты, связанные с реализацией данных технологий. Так, на данный момент рынок интеллектуального труда представлен, например, аналитическими компаниями (такими как *RAND* или *CNA*), занимающимися исследованиями социальных проблем, существующих в нашей стране, уязвимостей российской экономики, промышленности по инициативе американских и английских разведывательных служб. В российском сегменте отсутствуют организации, сравнимые с подобными мировыми аналитическими центрами. Россия находится на 38 месте в глобальном рейтинге аналитических центров военно-политической направленности, представленном в исследованиях ИМЭМО РАН [2].

Перечислим возможные направления применения существующих в нашей стране информационно-аналитических систем, способных противодействовать упомянутым исследованиям, апробированных, в основном, в практической деятельности органов внутренних дел (ОВД) России [3]. Использование подобных АПК не нарушает отечественного законодательства и может быть востребовано силовыми структурами и гражданами благодаря открытости и общедоступности размещаемой информации.

Первое направление связано с формированием центров анализа, решающих задачи по обеспечению разведывательной информацией руководства силовых структур, и инициировано тем, что в условиях ситуации ограниченных ресурсов для создания аналитических инструментов в этих структурах становится актуальным использование моделей частных военных компаний.

Центры анализа эффективно удовлетворяют запросы, вызванные необходимостью оценки террористических угроз, криминогенной обстановки, в том числе и в сфере IT-преступности, действий иностранных вооруженных сил у границ России, а также противостоят враждебным информационным кампаниям. Подход, основанный на функционировании частных аналитических центров, может решить некоторые бюрократические и финансовые проблемы: исследователями рассматриваются варианты создания «интеллектуальных объединений», которые будут действовать в условиях здоровой конкуренции для получения государственных контрактов с определенной целью повысить эффективность отмеченных видов деятельности.

Другое направление характеризуется использованием методов аналитической разведки *OSINT* (*Open Source INTelligence*). Это комплекс мероприятий, инструментов и методов, обеспечивающих получение и анализ бесплатной информации из открытых общедоступных источников, применяемых в отношении конкретных людей, организаций, а также событий, явлений [4].

OSINT оправдывает свою эффективность с первых лет существования. В 1941–1942 гг. специалисты анализировали фотоснимки парадов, опубликованные в немецких изданиях. Принципы работы технологии остались прежними, но инструменты и масштабы информации с тех пор существенно изменились [5].

Новые реалии жизни, функционирования человеческого общества обусловили освоение и киберпространства. В результате современный человек стал присутствовать как в материальном мире, так и в виртуальном – при помощи компьютерных устройств и систем коммуникации.

Любые действия людей в сфере информационных коммуникаций оставляют цифровые следы в виртуальном пространстве. Следовательно, сотрудники правоохранительных органов, раскрывая и расследуя правонарушения, могут и должны раз-

рабатывать и активно внедрять методы выявления и фиксации следов нового типа – присутствия участников происшествий и очевидцев в соответствующем сегменте виртуального мира, объективно связанном с географическим положением и общественной инфраструктурой. Особую значимость цифровые следы приобретают в ситуациях, когда первоначальные оперативные и следственные действия не привели к обнаружению или установлению участников, очевидцев и свидетелей правонарушений [6].

Цифровые следы, формирующиеся в виртуальном пространстве, фиксируются разнообразными электронными устройствами, в сферу действия которых попадает оставляющий их: мобильными телефонами без поддержки современных приложений; смартфонами с поддержкой приложений; ноутбуками, нетбуками, планшетами и иными малогабаритными компьютерами; электронными гаджетами (многофункциональными электронными часами, пульсомерами, шагомерами и т. д.); стационарными видеокамерами различных систем наблюдения, автомобильными регистраторами, GPS-навигаторами и др.

В деятельности оперативно-разыскных органов возникают и проблемы, связанные с использованием методики *OSINT*. Ее внедрение в работу всех оперативных подразделений ОВД и придание статуса приоритетного направления совершенствованию информационной основы являются важными шагами. Требуется также решение вопроса о деанонимизации в оперативной практике личности пользователей сети Интернет.

Третье направление, реализуемое в сфере применения информационно-аналитических систем, – обращение к возможностям разработанного и апробированного в 2016 г. российского программного комплекса «Поисковая система “СЕУС”» (ПС СЕУС), предназначенного для информационно-аналитического обеспечения оперативно-разыскной и разведывательной деятельности, противодействия распространению идеологии экстремизма и терроризма, иных деструктивных и противоправных явлений. В системе МВД России ПС СЕУС используется в основном сотрудниками центров «Э» и подразделений бюро специальных технических мероприятий (БСТМ) территориальных управлений более чем 20 регионов [3].

ПС СЕУС позволяет в автоматизированном режиме решать следующие оперативно-служебные задачи ОВД:

1. Выявление, предупреждение, пресечение, раскрытие и расследование преступлений, в том числе и IT-направленности, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших.

2. Розыск лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, а также розыск без вести пропавших.

3. Добывание информации о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности России, в сфере кибербезопасности и киберпреступности.

4. Установление имущества, подлежащего конфискации.

Знание методов сбора разведывательных, ориентирующих, доказательственных данных из открытых источников обязательно для профессионалов в области кибербезопасности. Интернет, социальные сети предоставляют богатые ресурсы для поиска информации о человеке: электронные адреса, телефоны, фотографии (в том числе с дополнительным анализом геолокации), личные сведения, информационные связи с друзьями, родственниками, объектами оперативного интереса и многое другое.

В контексте же работы, направленной на улучшение раскрываемости киберпреступлений, все большее значение приобретают возможности обращения к разноплановым сведениям, составляющим массив открытых данных о цифровых следах совершения противоправных деяний. Существующие и разрабатываемые методы способствуют эффективному формированию ориентирующей и процессуальной информации, создают уверенный информационный фон для раскрытия и расследования IT-преступлений. Совокупность специальных операторов и баз запросов современных аналитических систем упрощает этот процесс. Внедряемые технологии искусственного интеллекта все в большей степени обеспечивают поддержку проводимых аналитико-поисковых исследований, что особенно важно при обязательной обработке значительных по объему интернет-массивов, относимых к категории больших данных.

Список библиографических ссылок

1. Гаврилов А. М. Системы искусственного интеллекта в управлении полицией: опыт и проблемы // Безопасность и Право. 2020. № 15 (1). С. 78–92.

2. Умное оружие и мониторинг соцсетей: сможет ли ИИ предотвращать теракты // РБК: офиц. сайт. URL: https://trends.rbc.ru/trends/social/ 6169691a9a794774ed3f51d6 (дата обращения: 20.02.2025).

3. Противодействие экстремистской идеологии в социальных медиа: математические модели и методы: моногр. / К. М. Бондарь [и др.]. Хабаровск: РИО ДВЮИ МВД России, 2023. 232 с.

4. Дворянкин О. А. Osint, pentest и нетсталкинг – информационные технологии интернета // Национальная ассоциация ученых. 2022. № 84-2. С. 6–13.

5. Байжумаева М. А. Кибермошенничество // Новый юридический вестник. 2022. № 3 (36). С. 67–69.

6. Современное кибермошенничество: какие виды существуют и как им противостоять. URL: https://www.ixbt. com/live/offtopic/osnovy-kiberbezopasnosti-kak-zaschititsebya-i-svoi-dannye.html?ysclid=lpg3se7pju 30685616 (дата обращения: 26.02.2025).

Владислав Владимирович Булгаков,
курсант 532 учебного взвода 2 курса
Международно-правового факультета
Московского университета МВД России имени В. Я. Кикотя;
научный руководитель – Лариса Анатольевна Ларина,
заместитель начальника кафедры
конституционного и муниципального права
Московского университета МВД России имени В. Я. Кикотя,
кандидат юридических наук, доцент

ВЫЯВЛЕНИЕ ПРИЗНАКОВ ДИПФЕЙКА В ВИДЕОМАТЕРИАЛАХ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Высокие темпы роста производства цифрового контента и активное развитие видеоплатформ в информационно-телекоммуникационных сетях вызывают потребность в создании и применении технологий, способных обнаруживать фальсификацию видео.

Фальсификация видео представляет собой процесс, при котором оригинальный видеоматериал заменяется модифицированным, часто с целью получения возможности манипулирования кем-либо. Процесс может заключаться в создании ложных доказательств или искажении событий в политической сфере, а также в реализации других форм распространения дезинформации.

Количество ложных сообщений, зафиксированных в социальных сетях в течение 2023 г., превысило 12 млн. В совокупности они собрали миллиарды просмотров. За последние пять лет число киберпреступлений, составляющих сейчас почти 40 % от всех правонарушений, увеличилось более чем в два раза. С начала 2024 г. совокупный ущерб от таких преступлений достиг 116 млрд руб.

В последнее время получили широкое распространение видеоизображения, созданные с использованием технологии дипфейк, сгенерированные с помощью искусственного интеллекта.

Дипфейк – это технология, основанная на применении методов обработки видео- и аудиозаписей, использующая машинное и глубокое обучение для создания синтетических изображений, видео и аудио, имитирующих действия, происходящие в реальности. Это может быть наложение движений реального человека на движения выдуманного (нарисованного) персонажа, имитация движения воды, ветра, огня без использования их в реальности и т. п.

Основной принцип создания дипфейков – машинное и глубокое обучение, также известное как искусственный интеллект. Самой распространенной нейронной сетью, используемой для создания дипфейков, является генеративная состязательная сеть – GAN[1].

На ранних этапах развития технологий обработки изображений артикуляционная мимика и другие элементы синтезированных видео создавались в основном вручную. Процесс этот требовал огромных временных затрат и высокой квалификации специалистов, был медленным и трудоемким. Современные же технологии про-

[1] Основы генеративно-состязательных сетей. URL: https://habr.com/ru/articles/726254/ (дата обращения: 23.10.2024).

изводства дипфейков позволяют генерировать видео в режиме реального времени (real-time), значительно ускоряя изготовление «продукта» и открывая новые возможности для киноиндустрии, рекламы и даже для создания интерактивных виртуальных миров.

Дипфейк-технологии становятся все более доступными для мошенников, а преступные схемы последних – все более изощренными и трудными для распознавания. В условиях жизни современного информационного общества, для которого виртуальное взаимодействие стало нормой, жертвы нередко доверяют личностям, которых видят на экране, не подозревая о фальсификации изображения.

Кроме того, мошенники совершают свои действия на фоне состояний испуга, шока, вызываемых ими у жертвы. Часто их тактика включает создание экстренной ситуации. Так, просьба или требование перевести деньги под предлогом оказания срочной помощи вызывает у манипулируемого сильные эмоции и затрудняет его рациональное мышление. Находящиеся под давлением спешат выполнить просьбу, и это усугубляет последствия их «общения» с мошенниками.

В настоящее время в ряде случаев видеозаписи, созданные с использованием технологии дипфейк, содержат характерные визуально воспринимаемые признаки: неравномерное движение в кадре, несоответствие теней освещению, изменение освещенности в соседних кадрах видеозаписи, отсутствие моргания человека в кадре или моргание с одинаковой частотой; отсутствие синхронизации артикуляции губ человека с произносимой речью; наличие цифровых помех на видеоизображении и т. д.

По мере совершенствования технологий и качества изготовления дипфейк-изображений перечисленные признаки исчезнут. В настоящее время необходима разработка инструментов, которые позволят в автоматическом режиме осуществлять анализ видеопотока на предмет наличия признаков дипфейков.

Ключевые инструменты для решения этой задачи – сверточные нейронные сети (CNN), используемые для извлечения важных признаков из видеопотока, а также автокодировщики для детектирования аномалий и подмен в метаданных.

Важность обеспечения безопасности и достоверности видеоконтента возрастает на фоне широкого распространения технологий глубокого обучения и искусственного интеллекта, позволяющих манипулировать видеоматериалами и достигать высокой степени реалистичности произведенных записей, изображений и т. д., в то время как традиционные методы детектирования подмены (анализ метаданных, проверка физического происхождения видеоматериала и др.) могут быть весьма ограничены в возможностях выявления признаков изменения видеоматериалов.

Современные алгоритмы машинного обучения предлагают более точные и надежные методы для обнаружения подмены. Способность нейронных сетей не только анализировать визуальные элементы, но и выявлять скрытые аномалии в поведении объектов делает их незаменимыми в борьбе с фальсификациями. Однако те же технологии могут быть использованы и для создания фальшивых видеоматериалов. Это подчеркивает необходимость разработки эффективных систем защиты от подмен и фальсификаций видеопотока.

К таковым нам представляется возможным отнести систему, состоящую из двух основных компонентов.

Первый предполагает предварительную обработку видео с использованием машинного обучения. Все видео на старте анализируются с помощью методов компьютерного зрения: извлекаются важные метаданные. Для этого используются сверточные нейронные сети, которые обучаются на большом наборе данных для класси-

фикации и детекции объектов в видео. Каждый кадр видео проходит через сеть, где из него извлекаются значимые метаданные, такие как обнаруженные объекты, их местоположение.

Второй ориентирует на сравнение метаданных и видео. Метаданные сохраняются в JSON-формате и отправляются на сервер для дальнейшего анализа, который производится при помощи автокодировщика – особого типа нейронной сети, – обученного на задаче сжатия и восстановления данных. Этот анализ необходим для выявления отклонений в данных (если восстановленные данные сильно отличаются от оригинала, можно предполагать наличие аномалии). В нашем случае обучение осуществляется на метаданных доверенного видео и в дальнейшем мы можем сверяться с любым недоверенным. Результат сравнения состоит в том, что система при помощи автокодировщика детектирует аномалии и проверяет объекты на наличие расхождения между оригинальным и проверяемым видео.

Первый этап анализирует каждый кадр видео для обнаружения на нем объектов при помощи сверточной нейронной сети. Для этого используется заранее обученная модель. Далее кадр сохраняется в формате JSON и передается на следующую ступень системы для обучения автокодировщика.

В данную систему, реализованную на языке Python и JavaScript, можно загрузить два медиафайла и сгенерировать или загрузить (если они были сгенерированы ранее) существующие метаданные. После этого станет доступным анализ метаданных обоих видео. По окончании анализа при выявлении в процессе сопоставления ошибок можно перейти к тому времени, в которое они были обнаружены в обоих видео для визуального сравнения.

Такой подход, основанный на использовании сверточных нейронных сетей и автокодировщиков, позволяет значительно повысить точность и надежность системы, дающей возможность эффективно обнаруживать подмены в видеопотоке, что крайне важно в условиях растущей угрозы фальсификации видеоконтента. Система обеспечивает автоматическое выявление манипуляций с видеопотоками и защиту от распространения недостоверной информации.

Битва между создателями дипфейков и разработчиками технологий выявления фальсифицированного видео только начинается. Поддерживая баланс между стремлением к инновациям и ответственностью, человечество сможет более эффективно справляться с вызовами, которые бросают ему невидимые подделки в эру высоких технологий.

Библиографический список

1. Виноградов, В. А. Зарубежный опыт правового регулирования технологии «дипфейк» / В. А. Виноградов, Д. В. Кузнецова // Право. Журнал Высшей школы экономики. – 2024. – № 2. – С. 215–240.

2. Волкова, Г. Е. К вопросу о защите прав личности в условиях распространения дипфейк-технологий // Юристъ-Правоведъ. – 2023. – № 3 (106). – С. 15–22.

3. Исакова, А. Г. Применение искусственного интеллекта в расследовании преступлений с использованием технологии «дипфейк» / А. Г. Исакова, А. В. Осин // Вестник науки. – 2024. – Т. 3, № 1 (70). – С. 235–242.

4. Киселев, А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2021. – № 3. – С. 54–64.

5. Климова, Я. А. Криминалистический анализ преступлений, совершенных с использованием дипфейк-технологии // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2024. – № 2 (76). – С. 29–35.

Светлана Андреевна Дряглина,
преподаватель кафедры общеправовых дисциплин
Дальневосточного юридического института
МВД России им. И. Ф. Шилова

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Информационно-телекоммуникационные технологии значительно упростили жизнь современного человека и оказали существенное влияние на правоотношения, в которых он участвует. Научно-технический прогресс не всегда приносит только благо. Широкое распространение его достижений открыло новые возможности и для преступников.

Ежегодно количество зарегистрированных преступлений с использованием информационно-коммуникационных технологий возрастает. По мере развития технологий преступники изменяют, адаптируют к новым условиям механизмы совершения преступлений, изобретая новые способы воздействия на потерпевших.

За 2024 г. число преступлений с использованием информационно-коммуникационных технологий увеличилось на 12,9 % (с 668,7 тыс. до 755,1 тыс.), из них на 7,4 % – тяжких и особо тяжких (с 338,3 тыс. до 363,3 тыс.) [1]. Меняется структура таких преступлений, а методы их совершения становятся все более сложными. Это связано с постоянной эволюцией информационных технологий и компьютерных устройств, обладающих широким спектром функций, позволяющих анонимизировать данные личности в цифровом пространстве.

Преступления, совершаемые с использованием сети Интернет, не имеют национальных границ и, следовательно, являются трансграничными.

Транснациональная преступность – комплекс противоправных общественно опасных деяний, которые осуществляются и имеют последствия за пределами границ какого-либо государства. Они могут быть произведены в любом месте, находящемся на территории одного государства в отношении субъектов другого. Данные, содержащиеся в компьютерных системах, быстро уничтожаются, что позволяет преступнику скрывать следы преступления и избегать наказания за совершенное деяние.

Преступления транснационального (трансграничного) характера относятся, как правило, к категории тяжких или особо тяжких. Они посягают на мировой порядок, права и свободы человека, на взаимное сотрудничество государств в области экономики, культуры, торговли, следовательно, представляют глобальную опасность для развития и укрепления международных отношений [2, с. 10].

Проблемы, вызванные необходимостью оказания противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, в настоящее время приобрели глобальный характер. Наибольшую активность проявляют организованные преступные группы, располагающие возможностями применения вредоносного программного обеспечения, специальной техникой, сим-боксами, социальными сетями, фишинговыми сайтами, электронными платформами, колл-центрами, виртуальными АТС, осуществляющими мошеннические звонки с подменных номеров.

Следственные органы испытывают сложности уже на первоначальном этапе расследования таких преступлений, когда необходимо установить место совершения. К примеру, преступник предпринял DDoS-атаку на сервер компании. Необходимо определить, что будет являться местом совершения преступления с процессуальной точки зрения в данной ситуации: место написания программы, место пребывания преступника или иное место.

Некоторые исследователи считают местом совершения преступления «виртуальное пространство», в пределах которого происходит противоправное деяние. Принятие этой точки зрения вызывает новый вопрос: как осуществлять осмотр места происшествия в киберпространстве, если в данной ситуации применение тактических приемов осмотра места происшествия будет безрезультатным?

Некоторые авторы (например, Т. И. Денисова), анализируя судебно-следственную практику, приходят к тому, что в случае хищения, при совершении которого потерпевшим использовался стационарный компьютер, местом происшествия будет являться помещение, где находится данное устройство. Здесь тактически важно обратить внимание на следующие детали: расположение компьютера, наличие устройств телекоммуникации (роутера, модема), порядок их соединения (беспроводная связь, компьютерная сеть); назначение, название, серийный номер, комплектация данных устройств; содержание информации на мониторе; описание Интернет-ресурса, с помощью которого совершены противоправные действия. При расследовании хищения с использованием мобильного телефона следователь может определить в качестве места осмотра происшествия свой рабочий кабинет, что подтверждается следственной практикой [3].

К числу обстоятельств, существенно осложняющих борьбу с преступлениями рассматриваемой категории в условиях отсутствия системы эффективного процессуального использования цифровых следов для привлечения виновных к ответственности, относится возможность осуществлять посягательства из любой точки мира, воздействовать на большое количество людей, использовать средства анонимизации, криптовалюту, цифровые ресурсы, зарегистрированные в недружественных странах.

Для фиксации цифровых следов следователь не всегда обладает специальным аппаратным обеспечением и специализированными навыками. При назначении же экспертизы трудности возникают при постановке вопросов, адресованных эксперту.

Эффективность процедуры расследования определяется несколькими факторами: во-первых, качеством взаимодействия полиции России, ФСБ с правоохранительными органами иностранных государств, рядом неправительственных организаций, специализирующихся на противодействии преступлениям, связанным с использованием информационно-коммуникационных технологий; во-вторых, компетентностью следователей, экспертов и оперуполномоченных (понимание технологических характеристик компьютерных систем и программ, при помощи которых совершаются преступления, обеспечит появление представления о том, как работают, применяются те или иные технологии). Необходимо создать специализированные программы обучения (повышения квалификации) для специалистов, занимающихся расследованием преступлений, совершаемых с использованием информационно-коммуникационных технологий, привлечь к реализации этих программ теоретиков в области уголовного права и уголовного процесса, экспертов-криминалистов, экспертов-техников и специалистов в области компьютерной безопасности.

Список библиографических ссылок

1. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2024 года // Министерство внутренних дел Российской Федерации: офиц. сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 14.05.2025).

2. Трунцевский Ю. В. Понятие транснационального преступления // Международное уголовное право и международная юстиция. 2014. № 3. С. 9–12.

3. Денисова Т. А. Некоторые тактические особенности производства осмотра места происшествия при расследовании хищений, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика – наука без границ: традиции и новации: материалы Междунар. науч.-практ. конф. (30 ноября – 1 декабря 2023 г., Санкт-Петербург). СПб.: Изд-во Санкт-Петербургского университета МВД России, 2024. С. 620–624.

Игорь Викторович Едынак,
старший преподаватель кафедры информационного
и технического обеспечения органов внутренних дел
Дальневосточного юридического института
МВД России имени И. Ф. Шилова,

Арина Юрьевна Колесникова,
преподаватель кафедры информационного
и технического обеспечения органов внутренних дел
Дальневосточного юридического института
МВД России имени И. Ф. Шилова

АСПЕКТЫ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРАВОНАРУШЕНИЯ В СЕТИ ИНТЕРНЕТ

В современном информационном обществе Интернет – неотъемлемая часть повседневной жизни. Он предоставляет множество возможностей, в том числе доступ к необходимой информации, коммуникации с другими людьми, помогает в осуществлении иных видов деятельности. Однако также необходимо учитывать, что сеть Интернет может быть использована и для совершения правонарушений.

Выявление таких правонарушений – сложная задача, решение которой требует постоянного развития и совершенствования правовых механизмов и инструментов. Правонарушения, совершенные с использованием сети Интернет, могут принимать различные формы – от незаконного доступа к компьютерным данным и распространения вредоносного программного обеспечения до мошенничества, нарушения авторских прав и осуществления различных кибератак.

В постановлении Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”» указано: «Информационно-коммуникационные технологии являются основой стратегического развития в современном мире и неотъемлемой частью управленческих систем в ключевых отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка» [1].

В настоящее время существуют механизмы и методы, позволяющие обнаруживать и расследовать правонарушения, совершенные с помощью Интернета. Однако задача их расследования и пресечения остается сложной и актуальной из-за быстрого развития сети и появления новых технологий.

В выявлении и расследовании этих правонарушений должны участвовать не только сотрудники правоохранительных органов, но и специалисты в области информационных технологий и кибербезопасности, разрабатывающие методы обнаружения преступных действий, выполняющие экспертизу компьютерных данных и выявляющие следы преступного поведения в сети Интернет.

В ряде источников, авторы которых ссылаются на статистику Министерства внутренних дел, указано, что количество преступлений с использованием информационно-телекоммуникационных технологий в 2024 г. составило 40 % от общего числа преступлений, при этом в четырех из пяти случаев была использована сеть Интернет. Учитывая высокую латентность таких преступлений, можем предположить, что

реальное количество киберпреступлений значительно превышает указанное в официальной статистике [2].

Важной задачей является совершенствование законодательства в области Интернета и кибербезопасности. Страны во всем мире работают над созданием и усовершенствованием законов (о кибербезопасности, защите персональных данных, борьбе с киберпреступностью и т. д.), определяющих особенности регулирования пользования Интернетом и наказания за правонарушения, совершенные в нем. Разрабатываются соответствующие международные соглашения.

Для обеспечения правового регулирования и контроля над соблюдением законности в Интернете существует ряд основных нормативных актов, которые определяют административную ответственность за такие правонарушения.

Одним из наиболее значимых нормативных правовых документов в данной области является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3]. Он конкретизирует общие принципы регулирования в области информации и информационных технологий, а также устанавливает ответственность за распространение запрещенной на территории Российской Федерации информации.

Кодексом Российской Федерации об административных нарушениях [4] (далее – КоАП РФ) регулируется, соответственно, административная ответственность за правонарушения в Интернете. Содержащиеся в нем нормы предусматривают санкции для лиц, нарушающих законодательство в сфере информационных технологий и Интернета. К таким нарушениям относятся, например, распространение запрещенной информации, незаконный доступ к информационным ресурсам или создание вирусов и вредоносных программ.

В настоящее время для особенной части КоАП РФ разрабатываются актуальные изменения, имеющие отношение к правонарушениям с использованием сети Интернет. Например, правонарушение, которое было совершено посредством цифровых технологий, имеет выражение как в активном деянии, так и в пассивном, то есть в бездействии.

Разработка норм ответственности подразумевает учет положений различных иных нормативных правовых документов, включая Указы Президента Российской Федерации (например, «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [5]).

Следует отметить, что основные нормативные акты, регулирующие административную ответственность за правонарушения в Интернете, играют важную роль в обеспечении законности и общественной безопасности. Они позволяют контролировать и пресекать нарушения в сфере информационных технологий и Интернета, защищая права и интересы граждан и общества в целом. Дадим краткую характеристику данной ответственности.

До начала 1990-х годов злоупотребления, связанные с использованием компьютера, не представляли значительной опасности и не привлекали внимание правительственных или международных организаций. Однако постепенное увеличение количества случаев и убытков, вызванных такими действиями, привело к вмешательству Организации Объединенных Наций (ООН), которая взяла на себя проведение исследований организованной преступности, в том числе анализ проблемы компьютерных злоупотреблений, рассматриваемых как форма международной преступности. Позднее были разработаны иные рекомендации и нормативные акты правительственных и международных организаций. В минимальный перечень можно включить следующие категории правонарушений:

– компьютерное мошенничество;
– компьютерный подлог;
– несанкционированный доступ к компьютерной системе;
– компьютерный саботаж;
– незаконное воспроизведение полупроводников;
– уничтожение программ или компьютерных данных;
– компьютерное пиратство (киберсквоттинг);
– компьютерное подслушивание.

Установленная КоАП РФ на текущий момент ответственность за нарушения, совершенные с использованием сети Интернет, относится лишь к некоторым из указанных в перечне. Правоохранительным органам, Интернет-провайдерам и каждому пользователю Интернета важно представлять возможные угрозы, соблюдать правила безопасности и активно противостоять любым проявлениям Интернет-правонарушений, чтобы обеспечить безопасное и защищенное пребывание в онлайн-пространстве.

Таким образом, совершение правонарушений в Интернете диктует необходимость утверждения соответствующей превентивной регламентации административной ответственности как важного инструмента государственного регулирования, способного обеспечить сокращение противоправных деяний этого вида. Развитие данной формы противодействия должно соотноситься с динамичным изменением информационной среды и возникающими стремлениями осуществления правонарушений разной природы.

Пути совершенствования рассматриваемой административной ответственности должны быть, по нашему мнению, связаны с организацией соответствующего мониторинга массивов Интернета в целях выявления новых особенностей способов осуществления правонарушений. Кроме того, требуются проведение специализированных исследований, выработка методических рекомендаций по эффективному определению критериев вины лиц, совершающих правонарушения в сети Интернет, и, самое главное, по формированию средств и способов доказывания вины правонарушителей с учетом особенностей электронного характера анализируемой информации, нюансов ее выявления, фиксации, процессуального закрепления.

Проведенное исследование позволяет сделать определенные выводы. Во-первых, административная ответственность является важным инструментом регулирования правовых отношений в сети Интернет. Ее применение направлено на предотвращение правонарушений и обеспечение защиты интересов граждан и организаций. Во-вторых, практика применения административной ответственности за правонарушение в сфере Интернета активно развивается и совершенствуется в соответствии с изменениями информационной среды.

Остаются и нерешенные проблемы в данной области. В современных условиях, когда информационные технологии развиваются с огромной скоростью, возникают новые виды правонарушений, требующие законодательного регулирования и последующего применения административной ответственности. Также возникают сложности при определении и доказывании вины лица, совершившего правонарушение в сети Интернет.

Исследование показало, что административная ответственность является важным механизмом борьбы с правонарушениями в сети Интернет. Тем не менее требуются дальнейшие научные исследования, усовершенствования нормативных актов, которые обеспечат более эффективное применение этого инструмента. Развитие информационных технологий нуждается в непрерывном обновлении и совершенство-

вании законодательства, эффективно реагирующего на изменения в информационной среде и обеспечивающего безопасность граждан и организаций в сети Интернет.

Список библиографических ссылок

1. Об утверждении государственной программы Российской Федерации «Информационное общество»: постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Карташева В. В России в 2024 году зарегистрировали рост числа IT-преступлений // Парламентская газета: офиц. сайт. URL: https://www.pnp.ru/social/v-rossii-v-2024-godu-zare-gistrirovali-rost-chisla-it-prestupleniy.html (дата обращения: 25.05.2025).

3. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ (ред. от 12 декабря 2023 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

4. Кодекс Российской Федерации об административных правонарушениях: федер. закон от 30 декабря 2001 г. № 195-ФЗ (ред. от 31 июля 2025 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

5. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 1 мая 2024 г. № 250. Доступ из справ.-правовой системы «КонсультантПлюс».

Артем Витальевич Иванов,
доцент кафедры экономической безопасности,
финансов и экономического анализа
Московского университета МВД России имени В. Я. Кикотя,
кандидат экономических наук

СПОСОБЫ ВЫЯВЛЕНИЯ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СРЕДЕ

Легализация доходов, полученных преступным путем, представляет собой одну из самых острых и актуальных проблем современного мира. В результате данного процесса незаконно полученные средства приобретают вид законных. Это позволяет преступникам скрывать истинное происхождение финансов и свободно использовать в экономике.

В условиях глобализации и цифровизации проблема приобретает международный характер, так как преступные группы активно используют финансовые системы разных стран, офшорные зоны и сложные схемы для перемещения денег через границы.

Нелегальные финансовые потоки оказывают разрушительное воздействие на экономику, подрывая ее стабильность, создавая дисбаланс на рынках, способствуя росту коррупции и ухудшая инвестиционный климат. Более того, отмытые средства нередко используются для финансирования других преступлений, таких как торговля наркотиками, оружием, людьми или поддержка террористических организаций.

С развитием технологий появляются новые инструменты для легализации доходов. Особую роль в этом процессе играют криптовалюты. Их децентрализованная природа и высокий уровень анонимности значительно усложняют отслеживание транзакций и выявление незаконной деятельности.

По данным Европола, масштабы проблемы впечатляют: ежегодно только в Европе объем операций по отмыванию денег достигает 4–5 млрд $. Этот факт обращает внимание на необходимость международного сотрудничества и разработки эффективных мер борьбы с описываемым явлением.

Криптовалюты становятся важным инструментом на различных этапах движения преступных доходов: от расчетов за запрещенные товары и услуги до осуществления операций по легализации полученных средств. Преступные группы используют цифровые активы для распределения денежных средств между организаторами и участниками преступных сообществ. Это становится возможным благодаря анонимности и децентрализованному характеру криптовалют, делающим их особенно привлекательными для киберпреступников, поскольку такие транзакции сложно отследить или привязать к конкретным лицам.

На первом этапе криптовалюты используются для расчетов за незаконные товары (наркотики, оружие, фальшивые документы и т. д.) и услуги. Платежи в криптовалютах позволяют преступникам избежать контроля со стороны банковской системы и государственных органов, так как операции проходят вне традиционных финансовых институтов. Сделки чаще всего совершаются через теневые рынки даркнета, где криптовалюты выступают основным платежным средством. Это позволяет преступникам оперативно и безопасно проводить расчеты, не опасаясь раскрытия личности.

На втором этапе криптовалюты становятся инструментом легализации доходов. Преступники используют сложные схемы для запутывания следов происхождения средств. Один из популярных методов – так называемые криптовалютные миксеры или тумблеры, которые смешивают транзакции разных пользователей, создавая множество новых операций и скрывая оригинальные источники средств.

На третьем этапе криптовалюты используются для распределения средств внутри преступной сети. Благодаря глобальной доступности и высокой скорости транзакций участники преступных групп могут быстро получать свою долю независимо от географического положения, что особенно удобно для международных криминальных организаций, члены которых находятся в разных странах. Такие операции позволяют минимизировать риски перехвата средств правоохранительными органами или финансовыми регуляторами.

Стоит подчеркнуть, что клиентам, которые взаимодействуют с банком или пользуются его услугами посредством применения современных технологий без личного контакта, зачастую присваивается более высокий уровень риска, связанный с отмыванием преступных доходов.

Индикаторами подозрительности финансовых операций, связанных с потенциальным отмыванием денежных средств или другой незаконной деятельностью, могут служить различные факторы, позволяющие банкам и финансовым учреждениям оценивать риски и выявлять операции, требующие дополнительного анализа. На рисунке представлены ключевые признаки, которые могут косвенно указывать на подозрительный характер финансовой активности клиентов (рис. 1).

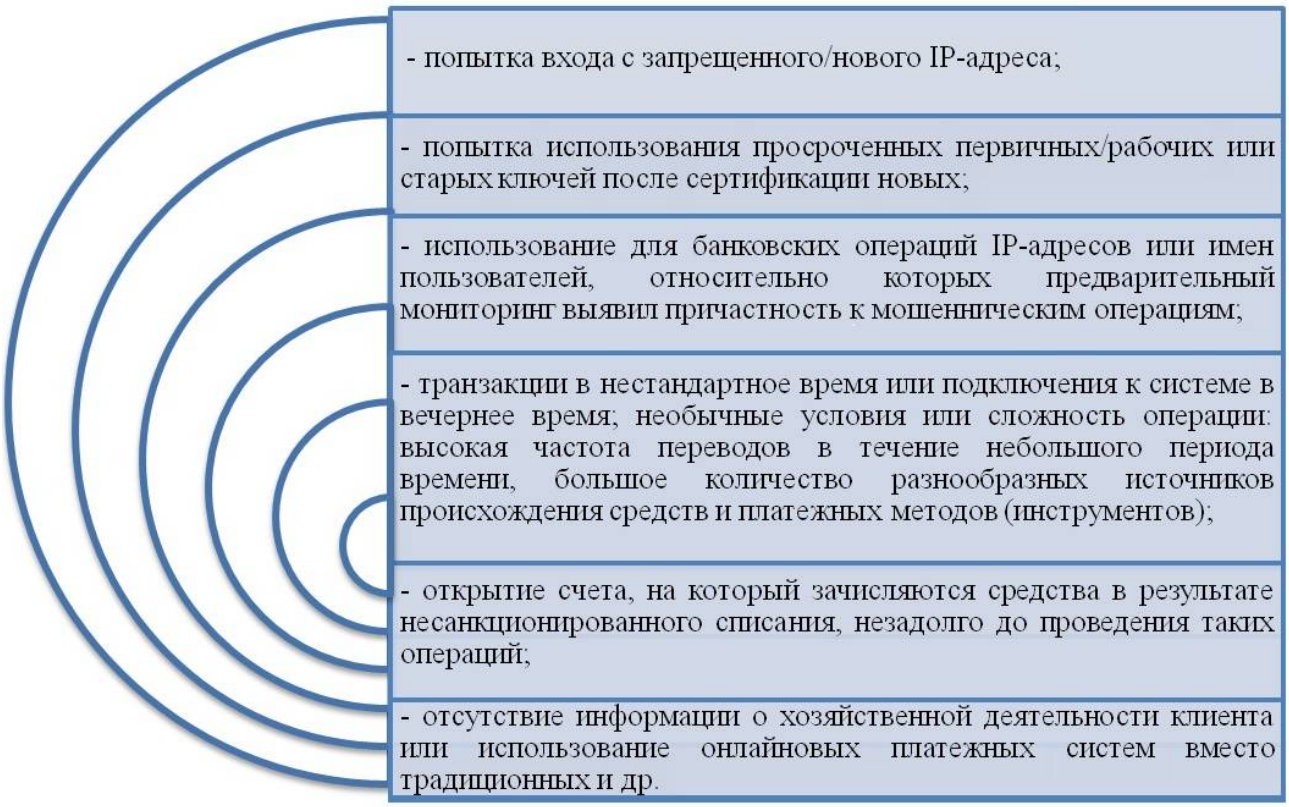

Рис. 1. Индикаторы подозрительности финансовых операций для банковских учреждений

Современная система взаимодействия с финансовыми институтами основывается на риск-ориентированном подходе. В России законодательство обязывает организации кредитно-финансового сектора передавать в финансовую разведку информацию о любых операциях, которые могут быть отнесены к категории повышенного риска, что позволяет Федеральной службе по финансовому мониторингу практически в режиме реального времени отслеживать всю финансовую активность в стране, включая ее динамику, проблемные области, а также деятельность отдельных финансовых институтов и секторов.

Отслеживание операций с криптовалютами, даже без привязки к конкретным владельцам кошельков, не представляет значительных трудностей благодаря открытости и прозрачности технологии блокчейн. Протокол блокчейна позволяет анализировать и отслеживать движение средств в сети. Для этого используются специализированные инструменты и сервисы, такие как Bitcoin Explorer, Insight, Cryptocurrency Alerting и другие, которые предоставляют доступ к информации о транзакциях [1].

Для усложнения процесса отслеживания криптовалютных операций пользователи могут обращаться к так называемым «микшерам» – посредническим сервисам, которые принимают средства от разных пользователей, смешивают финансы и возвращают участникам сети уже «очищенные» (то есть без прямой связи с исходными транзакциями) монеты. Таким образом, взаимодействие отправителя и получателя становится менее очевидным.

Еще одним методом сокрытия транзакций является применение протокола CoinJoin, который предполагает создание сложных «многокомпонентных» транзакций. В этом случае переводы нескольких пользователей объединяются в один платеж с множеством выходов. Это делает анализ транзакции более трудоемким для сторонних наблюдателей.

Использование таких инструментов, как микшеры или CoinJoin, хотя значительно затрудняет отслеживание операций, но не гарантирует полной анонимности. Технологии анализа блокчейна продолжают развиваться, что позволяет находить закономерности даже в сложных цепочках транзакций.

Следовательно, основная сложность в обеспечении прозрачности операций с криптовалютами заключается не столько в отслеживании самих транзакций, сколько в идентификации владельцев кошельков. Именно установление личности пользователя остается ключевой задачей для мониторинга и контроля операций в криптовалютной среде.

Предъявляемые государственной системе требования об оказании противодействия отмыванию денежных средств и финансированию терроризма с использованием криптовалют основываются на рекомендациях, подготовленных Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ). Данные международные стандарты задают рамки для формирования национальных систем финансового мониторинга [2].

Для традиционных субъектов первичного финансового мониторинга, таких как банки, страховые компании и другие финансовые организации, предусмотрен ряд обязательных мер, включающих идентификацию клиентов, выявление подозрительных операций и передачу соответствующей информации в подразделение финансовой разведки для дальнейшего анализа и расследования [1].

Однако стандартные подходы, используемые для контроля традиционных финансовых операций, не могут быть напрямую применены к криптовалютным транзакциям, что связано с особенностями технологии криптовалют – отсутствием

централизованных платежных систем, которые могли бы контролировать операции, и высокой степенью анонимности пользователей криптокошельков. Такие технологические свойства создают значительные сложности для мониторинга и требуют адаптации существующих механизмов противодействия отмыванию денежных средств и финансированию терроризма.

Государственные структуры получают возможность контролировать операции с криптовалютами, взаимодействуя с участниками криптовалютного рынка. Компании, работающие в этой сфере, обязаны соблюдать законодательство в области противодействия отмыванию денежных средств и финансированию терроризма. При соблюдении этого условия государство сможет отслеживать подозрительную активность и минимизировать риски использования цифровых активов в противоправных целях.

При отсутствии четко определенных критериев сомнительных операций массовый мониторинг неэффективен. Если критерии сформулированы неточно, большое количество ложных срабатываний значительно увеличивает нагрузку на аналитическое подразделение, что приводит к неоправданному увеличению сроков расследований; система мониторинга не позволяет выявить владельцев кошельков и бенефициаров цепочки транзакций для любой действующей в настоящее время криптовалюты, поскольку существуют криптовалюты, спроектированные таким образом, чтобы затруднить отслеживаемость операций. Рекомендуется обеспечить риск-ориентированный подход к созданию системы мониторинга криптовалютных транзакций, учитывающий инвестиционные затраты на создание системы мониторинга, текущие затраты на ее эксплуатацию и прогнозируемый эффект [1].

Список библиографических ссылок

1. Дурандина А. П. Государственная система мониторинга операций в криптовалюте // Инновации и инвестиции. 2021. № 2. С. 110–113.

2. Кондрат Е. Н. Международная финансовая безопасность в условиях глобализации. Основные направления правоохранительного сотрудничества государств: монография. М.: Юстицинформ, 2015. 592 с.

Анатолий Григорьевич Карпика,
доцент кафедры информационного обеспечения
органов внутренних дел
Ростовского юридического института МВД России,
кандидат технических наук, доцент

КЛАССИФИКАЦИЯ КИБЕРПРЕСТУПНИКОВ И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ

Расширение спектра и диверсификация стратегий и практики киберпреступности затрудняют определение уровня опасности, угрожающей обществу, и формирование эффективной политики профилактики кибербезопасности.

Первые исторические события, связанные с киберпреступностью, относятся ко времени возникновения компьютерных сетей, появления и развития рынка доступных персональных компьютеров. «Хакеры-пионеры» появились в Массачусетском технологическом институте в 1960 г., а первое публичное упоминание о них содержится в докладе, опубликованном в студенческом научном журнале The Tech: MIT Student Journal и датируется 20 ноября 1963 г. Первоначально термин «хакер» использовался для описания нестандартных действий, совершаемых при управлении и использовании компьютеров. Позднее он приобрел дополнительное значение: стал характеризовать и действия, наносящие ущерб информационным системам вообще и компьютерным – в частности. В 1978 г. Эйнар Стефферуд сообщил, что отправил первую рекламную рассылку в форме спама, содержащего рекламу нового компьютера компании DEC-10. Ее получателями стали владельцы почтовых адресов из списка агентства ARPANET [1].

Первой страной, принявшей закон о защите данных, была Швеция, составившая «Закон о данных 1973 года». В нем устанавливалось, что данные должны быть защищены от любого несанкционированного доступа. Аналогичный законодательный акт для наказания лиц, совершивших киберпреступления, затем был принят в США. Этот акт был ратифицирован как «Закон о защите Федеральных компьютерных систем 1977 года». Эти, на первый взгляд, изолированные – одно от другого – события имели решающее значение для создания компьютерной и цифровой криминалистики.

Первым киберпреступником, представшим перед судом 26 июля 1989 г. и приговоренным к наказанию в соответствии с «Законом о мошенничестве и преступном обращении с компьютером 1986 года», стал Роберт Моррис-младший – адъюнкт-профессор Массачусетского технологического института, известный как создатель первого сетевого червя, парализовавшего 2 ноября 1988 г. работу 6 200 компьютеров в США. Червь Морриса читал файл /etc/passwd операционных систем на ядре Linux, пытаясь подобрать пароли к учетным записям.

Сам термин «киберпреступность» был придуман в 1995 г. При этом указывалось, что явление не может быть описано единым определением, поскольку более целесообразно рассматривать его как набор действий, основанных на понятиях «материальное правонарушение» и «нарушение операций», влияющих на компьютерные данные или системы. Таким образом, сам термин описывает незаконные действия в отношении цифрового устройства, информации либо того и другого.

Исторически сложилось, что со временем термин «хакер» стал называть киберпреступника, и концептуализация деятельности хакеров стала, в основном, рассматриваться как мрачная, противозаконная, осуществляющаяся в подпольных условиях

с намерениями нанести ущерб информационным системам общества. Однако существует несколько категорий хакеров, деятельность которых различается.

СМИ и обычные люди относятся к хакерам как к несущим ответственность за проведение атак и повреждение компьютерных систем, однако хакерская онлайн-деятельность по преимуществу совершенно законна. Разница между хакерами, не совершающими преступления и совершающими их (киберпреступниками), состоит в отношении к закону, видах деятельности и мотивах. Анализ доступных источников позволил определить категории и классы хакеров.

«Белые шляпы» работают в соответствии с законом хакерской этики (не причинять вреда), иногда выступают в качестве экспертов по безопасности. «Серые шляпы» – реформированные «черные шляпы» – работают как консультанты по безопасности. «Черные шляпы» мотивированы жаждой наживы или ненавистью, у них отсутствуют представления о неэтичности кражи или уничтожения сетевых данных, полученных в результате несанкционированного доступа. В категориях «черных» и «белых» «шляп» принято выделять классы, отнесенность к которым определяет как уровень профессионализма хакера, так и мотивы сетевой активности. Элита обладает знаниями, навыками и опытом высшего уровня. Этот статус может быть получен благодаря созданию и применению особенно известного эксплойта, резонансному взлому или долговечности личной карьеры. Скрипт Киды – самый презираемый класс в более крупном хакерском сообществе. К ним, как правило, относят наименее квалифицированных и самых молодых участников, использующих инструменты, созданные элитными хакерами, сосредоточенных на количестве атак, а не на их качестве.

Кибертеррористы используют стеганографические и криптографические методы обмена информацией и специализируются на выведении из строя информационных систем и сегментов сети Интернет. Считаются наиболее серьезными киберпреступниками. Отдельная их «ветвь» – хакеры-самоубийцы, нацеленные на выведение из строя объектов критической инфраструктуры по радикальным причинам и не боящиеся попасть в тюрьму. К столь же опасной и наименее публичной группе лиц относятся недовольные бывшие сотрудники специализированных организаций, полагающие, что их недооценили или несправедливо уволили.

Сравнительно новой и быстрорастущей подгруппой хакеров являются хактивисты (наименование происходит от сочетания терминов «активность» и «взлом»). Они мотивированы на поддержку различных политических, религиозных и социальных течений и программ, и основными методами их деятельности являются атаки типа «отказ в обслуживании» сетевых ресурсов тех организаций, с деятельностью которых они выражают несогласие. Также стоит отметить хакеров-шпионов, заключающих контракты на проникновение и получение коммерческих секретов конкурентов их работодателя, а также создающих вредоносные программы и эксплойты, получающие сведения о негласно обнаруженных уязвимостях программного обеспечения.

Таким образом, киберпреступность является сложным и разнообразным по формам, мотивам и содержанию социальным явлением, которое эволюционирует вместе с обществом и технологиями. Распространение мобильных устройств, постоянно подключенных к компьютерным сетям, развитие нейронных сетей и открытости сети Интернет расширило спектр кибератак, стимулировало киберпреступность и связанную с ней кибервиктимизацию.

Жертвы киберпреступлений могут страдать от психологических и эмоциональных последствий, включающих посттравматическое стрессовое расстройство (ПТСР). Они также могут чувствовать стыд или переживать оскорбление (ввиду

вторжения в их частную жизнь), разрыв отношений из-за финансовых потерь, утечки информации, сексуального вымогательства или мошенничества при использовании ресурсов знакомств [2, с. 45].

Активный интерес киберпреступников ко многим сферам общественной деятельности и личной безопасности граждан обусловливает необходимость противостояния. Целесообразно начать с принятия личных мер защиты, далее распространить меры защиты на уровень организаций, общества, на корпоративный, национальный и международный уровни. Применение таких мер если не позволит гарантировать полную безопасность, то будет способствовать сведению к минимуму количества киберпреступлений, предотвращению большинства из них, значительному снижению ожидаемых злоумышленниками эффектов от кибератак.

Несомненно, самих по себе технологий защиты от киберпреступников и противодействия им недостаточно, требуется соединение усилий многих специалистов из разных областей, которые смогли бы реализовать соответствующее обучение, информирование, судебное преследование, международное сотрудничество, учитывая социальные аспекты, культурные традиции, основываясь на законодательстве.

Список библиографических ссылок

1. Cybercrime and cybercriminals a comprehensive study / R. Sabillon, V. Cavaller, J. Cano, J. Serra-Ruiz // International Journal of Computer Networks and Communications Security. 2016. № 4 (6). URL: https://www.researchgate.net/publication/304822458_ Cybercrime_and_Cybercriminals_A_Comprehensive_Study (дата обращения: 18.02.2025).

2. Карпика А. Г. Актуальные вопросы противодействия киберпреступлениям // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXVII Междунар. науч.-практ. конф. Красноярск, 4–5 апреля 2024 г. Красноярск: Сибирский юридический институт МВД России, 2024. С. 44–46.

Светлана Владимировна Лемайкина,
старший преподаватель кафедры
информационного обеспечения органов внутренних дел
Ростовского юридического института МВД России

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ ИНТЕРНЕТ ВЕЩЕЙ

Интернет вещей (далее – IoT) – это не просто модная технологическая концепция, а фундаментальное изменение принципов взаимодействия с окружающим миром. Его влияние пронизывает все аспекты нашей жизни от мелочей (таких как автоматическое включение освещения при входе в комнату) до глобальных изменений в управлении инфраструктурой городов и промышленности. IoT представляет собой колоссальную сеть взаимосвязанных устройств – от смартфонов и умных часов до промышленных датчиков, медицинского оборудования и автомобилей, каждое из которых способно собирать и передавать данные. Эта сеть не ограничивается наличием какого-то одного типа устройств: в ней сосуществуют миллиарды объектов, общающихся между собой и формирующих единую информационную среду. В основе IoT лежит концепция «умных устройств», оснащенных различными датчиками. Эти датчики измеряют параметры окружающей среды, физические характеристики объектов и даже биологические показатели. Информация, собираемая датчиками, бывает весьма разнообразной по формату и типу: это могут быть аналоговые сигналы, преобразуемые в цифровой формат, или непосредственно цифровые данные. Данные, собранные с бесчисленных устройств, поступают на платформы IoT – специализированные программные и аппаратные комплексы, обрабатывающие огромные объемы информации в режиме реального времени. Эти платформы отвечают за агрегацию, фильтрацию, хранение и анализ данных. В зависимости от сложности системы платформы IoT могут быть как облачными решениями, так и локальными системами.

История IoT началась в 1982 г. в университете Карнеги-Меллона, где была разработана автоматическая машина Coca-Cola, которая могла сообщать пользователю о статусе напитков, – первый прототип «умного устройства». В 1990 г. один из создателей протокола TCP/IP (на котором базируется работа всего Интернета) Джон Ромки привез свой домашний тостер на выставку технологий Interop и продемонстрировал публике причудливый эксперимент: он смог приготовить тост без прямого контакта с прибором: управление осуществлялось через удаленное подключение. Сам термин «Интернет вещей» (Internet of Things) был впервые предложен в 1999 г. Кевином Эштоном, использовавшим понятие для описания системы, в которой интернет служит средой взаимодействия не только для людей, но и для устройств, способных собирать данные и общаться друг с другом. С тех пор в мире наблюдается непрерывная интеллектуализация электронных устройств и технологий: телевизоров, телефонов, камер, термостатов, микрофонов, датчиков давления, датчиков уровня глюкозы, ЭКГ и многих других.

Сфера Интернета вещей, в силу своей природы, является технологически насыщенной и охватывает множество проводных и беспроводных протоколов, программных и аппаратных решений и, конечно, требует стандартизации и четкого определения правил взаимодействия составляющих ее частей. По прогнозам сайта Demandsage, в 2025 г. количество устройств Интернет вещей превысит 18 млрд, мировой рынок Интернет вещей достигнет 714,48 млрд $ [1]. Исследовательская

компания Machina Research опубликовала ежегодный отчет по росту рынка IoT, где отмечается, что общее количество IoT-подключений возрастет от 6 млрд по итогам 2015 г. до 27 млрд в 2025 г. [2]

Эта технология предоставляет обществу неоспоримые преимущества, автоматизируя процессы, повышая их эффективность и предоставляя новые возможности в самых разных областях – от управления умным домом до оптимизации промышленных производств и развития «умных» городов. Однако со стремительным распространением IoT появляются беспрецедентные вызовы для кибербезопасности, требующие глубокого понимания ситуации и комплексного подхода к защите. В отличие от традиционных компьютерных систем, IoT-устройства часто имеют ограниченные вычислительные ресурсы, упрощенное программное обеспечение и, что самое важное, слабую защиту. Это делает их привлекательной целью для киберпреступников. Спектр угроз, связанных с IoT, невероятно широк и расширяется постоянно.

Рассмотрим некоторые из наиболее распространенных угроз информационной безопасности IoT.

1. Атаки на основе уязвимостей. Многие IoT-устройства работают на устаревшем программном обеспечении с известными уязвимостями, не устраненными производителями. Это открывает «заднюю дверь» для хакеров. Так, уязвимости в протоколах связи (например, незащищенные протоколы HTTP, Telnet), неисправности в реализации криптографических алгоритмов или ошибки в коде самого устройства могут быть использованы для несанкционированного доступа. Эксплойты для таких уязвимостей часто оказываются в открытом доступе в даркнете, что упрощает задачу злоумышленников.

2. Атаки с использованием слабых паролей и учетных данных. У многих пользователей IoT-устройства имеют стандартные или легко угадываемые пароли. Эта практика значительно упрощает задачу злоумышленников, обращающихся к брутфорс-атакам или словарям для подбора паролей. Отсутствие многофакторной аутентификации (MFA) также существенно ухудшает безопасность.

3. Атаки типа «человек посередине» (Man-in-the-Middle, MITM). Злоумышленник может перехватить связь между IoT-устройством и сервером, модифицируя или перехватывая передаваемые данные. Это особенно опасно, если устройство передает конфиденциальную информацию, например, данные банковской карты или медицинские данные. MITM-атаки часто осуществляются путем создания фальшивой точки доступа Wi-Fi, к которой подключается устройство.

4. DDoS-атаки с использованием ботнетов. IoT-устройства, зараженные вредоносным ПО (часто через вышеупомянутые уязвимости), могут быть объединены в ботнет – распределенную сеть зараженных устройств, управляемых одним злоумышленником. Ботнет может использоваться для проведения DDoS-атак, перегружающих целевые серверы или сети трафиком, что приводит к их недоступности. Масштабы таких атак бывают огромными, если в ботнет вовлечены миллионы устройств.

5. Подмена данных (Data Tampering). Злоумышленник способен изменять данные, передаваемые или хранящиеся IoT-устройствами. В промышленных системах это может привести к сбоям в работе оборудования, авариям и материальному ущербу. В случае манипуляции данными в медицинских устройствах – к катастрофическим последствиям для здоровья пациентов. Например, изменение показаний датчиков в системе управления химическим процессом может привести к взрыву или утечке опасных веществ.

6. Физический доступ и клонирование. Некоторые IoT-устройства уязвимы для физического доступа. Злоумышленник получает доступ, изменяет настройки устройства, может установить на него вредоносное ПО или даже скопировать его функциональность.

7. Атаки на основе уязвимостей в облачных сервисах. Многие IoT-устройства взаимодействуют с облачными платформами для хранения и обработки данных. Уязвимости в этих облачных сервисах могут быть использованы для компрометации IoT-устройств и получения доступа к данным.

Произведенный анализ проблем позволяет сделать вывод о том, что борьба с киберугрозами в постоянно расширяющемся IoT-пространстве приобретает все более критическое значение. Система IoT, пронизывающая практически все сферы человеческой деятельности – от здравоохранения и транспорта до энергетики, финансов и сельского хозяйства, – стала невероятно уязвимой для злоумышленников. Многие страны стали применять разнообразные стратегии в борьбе с киберугрозами IoT. В США, например, Национальный институт стандартов и технологий (NIST) разрабатывает и публикует руководства и стандарты по безопасности IoT-устройств. Эти рекомендации имеют широкий спектр применения – от безопасного проектирования устройств и надежного управления паролями до реализации надежных механизмов обновления программного обеспечения [3]. Законодательные инициативы, такие как Закон об улучшении кибербезопасности IoT (IoT Cybersecurity Improvement Act), обязывают федеральные агентства применять минимальные стандарты безопасности при закупке и использовании IoT-устройств [4]. Кроме того, в США активно развиваются программы по повышению осведомленности граждан о кибербезопасности, организуются обучающие курсы для специалистов в области IoT-безопасности. В законодательном акте Европейского Союза (далее – ЕС) «Общий регламент по защите данных» (GDPR), который ориентируется на защиту пользователей, сформулированы жесткие требования к обработке персональных данных, полученных с помощью IoT-устройств. Это побуждает производителей уделять особое внимание конфиденциальности и безопасности [5]. Регуляторные органы ЕС активно контролируют соблюдение GDPR, налагая значительные штрафы за нарушения. Кроме того, ЕС инвестирует в исследования и разработки в области кибербезопасности, поддерживая создание инновационных решений для защиты IoT-экосистем. В Великобритании правительство опубликовало руководство для производителей IoT, содержащее рекомендации по обеспечению безопасности устройств на всех этапах жизненного цикла – от проектирования до утилизации. Этот документ включает в себя обязательные требования к использованию уникальных паролей, обеспечению поддержки обновлений безопасности и защите от распространенных уязвимостей. Правительство активно сотрудничает с отраслевыми организациями и исследовательскими центрами, чтобы создать более безопасную среду для развития IoT [6]. Китай, являющийся одним из мировых лидеров в области производства и внедрения IoT-устройств, активно разрабатывает национальные стандарты безопасности. Значительные инвестиции направляются на развитие искусственного интеллекта для мониторинга киберугроз и анализа больших данных, что позволяет выявлять и предотвращать атаки на ранних этапах. Кроме того, китайские власти стимулируют развитие кибербезопасности, создавая государственные программы и инвестируя в подготовку специалистов. Австралийское правительство разработало принципы безопасности IoT, ориентированные на производителей и поставщиков. К защите данных, системе обновления программного обеспечения и прозрачности в отношении обработки персональных данных предъявляются минимальные требования. Акцент делается на сотрудничестве между правительством, промышленностью и исследовательскими

институтами, способствующем созданию безопасной и надежной IoT-инфраструктуры [7]. В последние годы Россия активно внедряет технологии Интернета вещей (IoT) и Промышленного Интернета вещей (IIoT) в различные сферы общественной жизни и экономики, что оказывает влияние на цифровизацию как бытовых, так и промышленных процессов. Одной из ключевых областей применения IoT стал умный дом – технология, позволяющая автоматизировать управление устройствами и службами в жилых помещениях. Интерес к умному дому все активнее проявляют как пользователи, так и эксперты, что объясняется их стремлением к повышению качества жизни и эффективности управления домохозяйствами. В 2023 г. в России появился национальный стандарт, устанавливающий общие положения в области проектирования, применения, типовой структуры, интерфейсов и состава систем умного дома, а также их совместимости с внутренними и внешними системами [8].

Глобальная борьба с киберугрозами IoT требует непрерывных усилий со стороны правительств, промышленности и научного сообщества. Только комплексный подход, включающий разработку и внедрение международных стандартов, активное использование передовых технологий, повышение уровня киберграмотности населения и международное сотрудничество, позволит обеспечить безопасное и надежное функционирование Интернета вещей в будущем. В противном случае риск масштабных кибератак и серьезных последствий для критически важной инфраструктуры будет оставаться высоким.

Список библиографических ссылок

1. Kumar N. Internet of Things (IoT) Statistics: Market & Growth Data. URL: https://www.demandsage.com/internet-of-things-statistics/ (дата обращения: 17.02.2025).

2. Количество IoT-подключений вырастет в 2025 году до 27 млрд // iot.ru Новости Интернета вещей: офиц. сайт. URL: https://iot.ru/riteyl/kolichestvo-iot-podklyucheniy-vyrastet-v-2025-godu-do-27-mlrd- (дата обращения: 17.02.2025).

3. Джонсон З. GDPR и новые проблемы для IoT // iot.ru Новости Интернета вещей: офиц. сайт. URL: https://iot.ru/promyshlennost/gdpr-i-novye-problemy-dlya-iot (дата обращения: 17.02.2025).

4. Internet of Things Cybersecurity Improvement Act // The IT Law Wiki // Fandom. URL: https:// itlaw.fandom.com/wiki/Internet_of_Things_Cybersecurity_Improvement_Act (дата обращения: 17.02.2025).

5. NIST разрабатывает стандарты безопасности для IoT. // SecurityLab.ru: офиц. сайт. URL: https://www.securitylab.ru/news/491651.php (дата обращения: 17.02.2025).

6. Британские власти выпустили руководство по безопасности IoT-устройств // SecurityLab.ru: офиц. сайт. URL: https://www.securitylab.ru/news/495955.php (дата обращения: 17.02.2025).

7. Coker J. Australia Introduces Code of Practice for the Manufacture of IoT Devices // Infosecurity Magazine. URL: https://www.infosecurity-magazine.com/news/australia-code-of-practice-iot/ (дата обращения: 17.02.2025).

8. Хомяков Э. Г. Устройства умного дома и их значение при расследовании преступлений // Вестник Удмуртского университета. Серия «Экономика и право». 2025. Т. 35. Вып. 1. С. 166–173. URL: https://cyberleninka.ru/article/n/ustroystva-umnogo-doma-i-ih-znachenie-pri-rassledovanii-prestupleniy (дата обращения: 17.02.2025).

Илона Анатольевна Макаренко,
заведующий кафедрой криминалистики
Уфимского университета науки и технологий,
доктор юридических наук, профессор

Зарина Ирековна Харисова,
доцент кафедры криминалистики
Уфимского юридического института МВД России,
кандидат технических наук, доцент

О ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИХ СРЕДСТВАХ, ПРИМЕНЯЕМЫХ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Преступления в сфере компьютерной информации – это законодательное определение преступных деяний, предусмотренных гл. 28 Уголовного кодекса Российской Федерации (далее – УК РФ), объединяющей ст. 272, 272.1, 273, 274, 274.1, 274.2. В настоящее время наблюдается существенное увеличение количества преступлений, связанных с неправомерным доступом к охраняемой законом информации (ст. 272 УК РФ), ростом утечек конфиденциальных данных, способных нанести ущерб объектам критической информационной инфраструктуры Российской Федерации (ст. 274.1 УК РФ), хищением персональных данных граждан, их неправомерным использованием и распространением (ст. 272.1 УК РФ), противоправным применением информационно-телекоммуникационных технологий организованными преступными группами, которые все чаще используют вредоносное программное обеспечение (ст. 273 УК РФ), нарушением правил эксплуатации технических средств и информационно-телекоммуникационных сетей (ст. 274 УК РФ), а также нарушением правил централизованного управления средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети «Интернет» и сетей связи (ст. 274.2). Необходимо создать надежный барьер, препятствующий совершению преступлений именно в сфере компьютерной информации, выявить актуальные на сегодняшний день технико-криминалистические средства (далее – ТКС), применяемые при расследовании таких преступлений.

Значимость выявления способа – одного из важнейших элементов механизма совершения преступления в сфере компьютерной информации – обусловлена необходимостью установления следовой картины. Данный элемент весьма специфичен, поскольку в рассматриваемом виде преступлений, как правило, преобладают цифровые (электронные) следы. Свойство отражения, присущее всем видам и формам материи, заключается в том, что каждый объект материального мира в процессе взаимодействия с окружающей средой подвергается воздействию внешних факторов [1, с. 12]. Известно, что отражение присутствует всегда при взаимодействии двух и более материальных объектов – объектов следообразования. Поэтому основой для распознавания способа совершения преступления в сфере компьютерной информации служит следовая картина – отчасти в виде материальных, но все чаще в виде цифровых следов, идентифицируемых ТКС.

Применение того или иного ТКС определяет технико-криминалистический и тактико-криминалистический (тактический) приемы. Соответственно, для решения той

или иной криминалистической задачи выбирается наиболее эффективное ТКС [2], позволяющее достигнуть наилучших результатов расследования в оптимальные сроки, что соотносимо с основными специальными задачами криминалистики как науки. К числу ее дополнительных специальных задач относят: привлечение данных естественных и технических наук в целях оптимизации научно-технического обеспечения раскрытия и расследования преступлений; совершенствование имеющихся ТКС и применяемых тактических приемов, методических рекомендаций; анализ практики с целью выявления потребностей в новых ТКС, а также установления степени надежности и перспективности тех, которые были ранее рекомендованы к внедрению [3, с. 37].

Созданные или приспособленные для решения криминалистических задач средства в узком смысле определяют криминалистическую технику, которая занимается вопросами разработки понятийного аппарата и классификаций объектов исследования и их признаков. Так, например, на основе проведенной классификации папиллярных узоров возможно применение средств криминалистической идентификации, а на классификации внешних признаков человека базируется метод словесного портрета [3, с. 247].

Классификация, являясь основой таксономии (учения о принципах и практике систематизации сложноорганизованных сущностей), играет особую роль в развитии любой дисциплины. В криминалистике систематизация знаний о ТКС определяет эффективность системы противодействия преступности [4]. При рассмотрении преступлений в сфере компьютерной информации возможна систематизация знаний методом «от обратного»: допустимо выявить применимость того или иного ТКС на основе имеющихся представлений о свойствах цифровых доказательств. Этим объясняется целесообразность выявления и систематизации современных ТКС, использование которых позволит определить наиболее эффективную тактику подготовки и проведения отдельных следственных действий исходя из складывающихся по преступлению в сфере компьютерной информации обстоятельств.

ТКС включают широкий круг аппаратных, программно-аппаратных и программных средств, которые могут быть классифицированы по различным основаниям. Это предполагает возможность построения различных взаимосвязанных классификаций, исходящих из разных криминалистически значимых классификационных критериев [5, с. 437].

Существующие ТКС, применение которых целесообразно при расследовании преступлений в сфере компьютерной информации, можно классифицировать по характеру воздействия на информацию, уровню автоматизации расследования, источнику получаемой информации, цели применения и функциональному назначению.

Так, по характеру воздействия на информацию ТКС подразделяются на

– пассивные, не оказывающие воздействия на исследуемую криминалистически значимую компьютерную информацию и направленные на поиск и исследование существующих данных (анализ сетевого трафика, дампов памяти, мониторинг веб-ресурсов и пр.),

– активные – предполагающие непосредственное воздействие на исследуемую информацию с целью проверки выдвинутых версий (динамический анализ вредоносного кода, внедрение сетевых ловушек и пр.),

– комбинированные – сочетающие возможности как активных, так и пассивных средств (использование сетевых анализаторов для пассивного сбора трафика с последующим активным анализом полученных данных [6, с. 12] и т. п.).

По уровню автоматизации расследования преступления в сфере компьютерной информации выделяются следующие ТКС:

– неавтоматизированные – требующие для выполнения действий участия следователя или специалиста (ручной анализ лог-файлов, исследование исходного кода вредоносных программ и т. п.),

– автоматизированные – действующие на базе программного обеспечения, функционирующего по настраиваемому пользователем алгоритму (избирательное восстановление удаленных файлов и их последующий анализ и т. п.),

– автоматические – действующие на базе программных средств, функционирующих по заранее определенному жесткому алгоритму (это могут быть SIEM-системы («security information and event management – система управления информационной безопасностью и событиями безопасности») [7, с. 1022] или антивирусное программное обеспечение, используемое для обнаружения вредоносных объектов и пр.).

По источнику получаемой информации выделяются ТКС, производящие анализ

– криминалистически значимой информации в компьютерах, мобильных средствах связи, серверных станциях и других устройствах [8, с. 3] (анализ файловой структуры, реестра операционной системы устройства и пр.),

– сетевого трафика или предполагающие получение данных из информационно-телекоммуникационной сети, протоколов обмена файлами и т. д. (захват и анализ сетевого трафика с помощью снифферов, анализ DNS-запросов и пр.),

– данных из облачных хранилищ, необходимых для получения сведений из удаленно расположенных серверов (анализ активности пользователей в облачном хранилище поставщика услуг средствами специализированного программного обеспечения и т. п.),

– сведений из общедоступных баз данных и ресурсов сети Интернет (OSINT-разведка (англ. – «open source intelligence» – инструменты для получения и анализа информации из открытых источников) [9, с. 131]).

По цели применения можно рассматривать ТКС, предназначенные для

– идентификации преступника (выявление IP-идентификатора или MAC-адреса пользователя, метаданных файлов и пр.),

– установления факта совершения преступления (подтверждение факта несанкционированного доступа к компьютерной информации или распространения вредоносного программного обеспечения путем анализа лог-файлов или сетевого трафика),

– определения нанесенного ущерба (анализ финансовых транзакций или простоя технологического оборудования).

По функциональному назначению можно выделить ТКС, применяемые для

– создания образов носителей информации и дампов памяти для их последующего анализа,

– анализа файловых систем (исследование структуры и содержимого системы организации, хранения и именования данных на носителях информации),

– захвата и исследования сетевого трафика для выявления аномалий и вредоносной активности [10, с. 122],

– анализа лог-файлов (поиск, собирание и анализ информации о работе технических средств или программного обеспечения) [11, с. 3],

– восстановления данных,

– визуализации данных (отображение в наглядной форме взаимосвязей с целью выявления закономерностей и пр.).

Таким образом, рассматриваемые ТКС представляют собой, преимущественно, совокупность программных и аппаратных инструментов поиска и анализа цифровых доказательств. Практическая значимость приведенных классификаций определяется необходимостью систематизации знаний об имеющихся на сегодняшний день ТКС, применяемых при расследовании преступлений в сфере компьютерной информации. Четкое представление об особенностях и системных связях ТКС облегчает их поиск и выбор для решения конкретных задач, формулирование принципов использования, определения критериев их подбора к конкретному виду преступного деяния, стимулирование разработки инструментов, направленных на противодействие вновь возникающим киберугрозам, а также стандартизацию применения указанных средств в процессе сбора цифровых доказательств и обеспечения их допустимости в суде.

Список библиографических ссылок

1. Вехов В. Б., Смагоринский Б. П., Ковалев С. А. Электронные следы в системе криминалистики // Судебная экспертиза. 2016. № 2 (46). С. 10–19.

2. Josang A. Cyber Organizational Structures and Regulation // Cybersecurity. URL: https://link.springer.com/chapter/10.1007/978-3-031-68483-8_17 (дата обращения: 17.03.2025).

3. Курс криминалистики. В 3 т. Т. I. Общая теория криминалистики. Криминалистическая техника. Криминалистическая тактика: учебник / А. Н. Басалаев, В. С. Бурданова, М. Б. Вандер [и др.]. СПб.: Издательство «Юридический центр Пресс», 2024. 726 с.

4. Таксономия // Большая советская энциклопедия. URL: https://gufo.me/dict/bse/Таксономия (дата обращения: 14.04.2025).

5. Поляков В. В. Криминалистическая классификация средств высокотехнологичных преступлений // Вестник Санкт-Петербургского университета. Право. 2024. Т. 15. Вып. 2. С. 435–453.

6. Challenges of criminal investigation cybercrime / W. Hartono, D. Muhardi, A. Akhiruddin, D. V. B. Purba, P. Asa, Y. Dm // Awang long law review. 2024. Vol. 7, № 1. P. 11–19.

7. Jajodia S., Samarati P., Yung M. SIEM System // Encyclopedia of cryptography, security and privacy. Cham: Springer, 2025. 2412 p.

8. Cybercrime in the era of mobile and wireless devices / C. K. Gomathy, V. Geetha, S. T. Ramacharla, A. Vustepalle // International journal of scientific research in engineering and management. 2024. Vol. 8, № 9. P. 1–4.

9. Roberts A. The Importance of OSINT. Cyber threat intelligence. Berkeley: Apress, 2021. P. 131–152.

10. Classifying cybercrime networks: organized and transnational schemes in the digital era / I. Tiutiunyk, D. Toptunenko, A. Flaumer // Socio-Economic Relations in the Digital Society. 2024. Vol. 3, № 53. P. 121–129.

11. Legal frameworks for regulating cybercrime and cyber terrorism / C. K. Gomathy, P. V. Rajesh, D. S. Manohar, V. Geetha // International journal of scientific research in engineering and management. 2024. Vol. 8, № 9. P. 1–7.

Антон Владимирович Матвеев,
преподаватель кафедры специальных дисциплин
Ленинградского областного филиала
Санкт-Петербургского университета МВД России,
кандидат юридических наук

ДОКАЗАТЕЛЬСТВА ПО ДЕЛАМ О СКЛОНЕНИИ К ПОТРЕБЛЕНИЮ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ ИЛИ ИХ АНАЛОГОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ: ВИДЫ И ХАРАКТЕРИСТИКА

В современном мире информационно-телекоммуникационные сети, включая сеть Интернет, стали основным инструментом для совершения преступлений, связанных с незаконным оборотом наркотических средств. В последнее время преступники все чаще используют сеть Интернет для совершения преступлений, связанных со склонением к потреблению наркотических средств. Уголовная ответственность за склонение к потреблению наркотических средств, психотропных веществ или их аналогов с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», предусмотрена п. «д» ч. 2 ст. 230 Уголовного кодекса Российской Федерации [1] (далее – УК РФ). У столкнувшейся с этими новыми вызовами правоохранительной системы России возникла необходимость выявления, фиксации и анализа доказательств в цифровой среде.

В научно-юридическом контексте состав преступления, предусмотренный ст. 230 УК РФ, характеризуется совершением умышленных действий, направленных на формирование у третьих лиц намерения к употреблению наркотических средств, психотропных веществ либо их аналогов. Криминообразующие признаки деяния могут проявляться в активной форме (убеждение, предложение, рекомендации) в реализации противоправных методов воздействия (включая введение в заблуждение, применение психического или физического принуждения, лишение свободы действий). При этом законодатель не устанавливает требования к систематичности противоправного поведения: для квалификации достаточно однократного эпизода склонения.

Особенностью объективной стороны состава является отсутствие необходимости достижения фактического результата: преступление признается оконченным в момент совершения противоправных действий независимо от того, реализован ли адресатом навязанный поведенческий сценарий. Данная правовая конструкция ориентирована на превентивную защиту общественных отношений, акцентирована ответственность за факт создания условий, потенциально опасных для здоровья населения [2].

Одним из ключевых доказательств по делам о склонении к потреблению наркотических средств, психотропных веществ или их аналогов с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, является электронная переписка между обвиняемым и потерпевшим, полученная, например, из мессенджеров (например, Telegram, WhatsApp[1]) или социальных сетей и содержащая предложения, уговоры, описание ощущений, вызываемых употреблением наркотических средств, а также договоренности о встрече для совместного употребления. Так,

[1] Принадлежит компании Meta, которая признана экстремистской и запрещена в РФ.

согласно приговору Кировского районного суда г. Уфы от 13 августа 2024 г. по делу № 1–325/2024, обвиняемый, являясь потребителем наркотического вещества, действуя с прямым умыслом, осознавая общественную опасность своих действий, через социальную сеть Telegram (разместив в группе объявление) связался с потерпевшей, которую решил склонить к потреблению наркотического вещества. Обвиняемый, дождавшись прибытия по месту его проживания потерпевшей, умышленно, используя ранее приобретенное наркотическое вещество, действуя путем предложения с целью склонения потерпевшей к потреблению наркотического вещества, возбудил у нее интерес и желание потребить наркотическое вещество. В качестве одного из доказательств вины в совершенном преступлении суд использовал скриншот сообщений в группе в мессенджере Telegram, на котором отражено сообщение обвиняемого с предложением потребить наркотическое вещество [3].

В некоторых случаях суды принимают в качестве доказательств аудио- и видеосообщения, отправленные обвиняемым потерпевшему. В таких сообщениях могут содержаться уговоры, описание ощущений, вызываемых употреблением наркотиков, а также демонстрация процесса употребления. Так, из приговора Октябрьского районного суда г. Кирова от 31 марта 2023 г. по делу № 1-167/2023 следует, что обвиняемый, находясь в своей квартире, решил в ходе Интернет-переписки склонить знакомую к совместному потреблению наркотического средства. Реализуя задуманное, осознавая противоправность совершаемого деяния, обвиняемый в программе мгновенного обмена сообщениями Telegram посредством текстовых, собственных голосовых сообщений и видео из сети Интернет путем уговоров, предложений, а также видео-демонстрации и описания эффекта воздействия наркотика на организм возбудил у своей знакомой желание потребить наркотическое средство. Обвиняемый достиг ожидаемого результата, вызвав у женщины желание испытать наркотическое опьянение и состояние эйфории. Таким образом, своими активными умышленными действиями в сети Интернет (уговорами, описанием эффекта воздействия наркотика на организм, предложением потребить наркотическое вещество) обвиняемый, используя сеть Интернет, склонил знакомую к потреблению наркотических средств [4].

Скриншоты переписок, фотографии наркотических средств, изображения, подтверждающие факт передачи наркотиков, также признаются судами в качестве доказательств. Например, в апелляционном определении Самарского областного суда от 19 июня 2024 г. по делу № 22-2546/2024 суд принял в качестве доказательства скриншоты переписки, в которой обвиняемый предлагал потерпевшей потребить наркотическое средство. Так, из показаний потерпевшей следует, что обвиняемый несколько раз предлагал ей потребить наркотик совместно, присылал аудиосообщения и фотографии пакетика с веществом белого цвета. В какой-то момент она, под воздействием преследования обвиняемого и своего психического состояния, согласилась на предложение, чтобы знакомый оставил ее в покое. Исследованное судом содержание переписки в телефонах потерпевшей и обвиняемого, показания потерпевшей подтверждают, что именно обвиняемый был инициатором переписки, сообщал о наличии у него наркотического средства, которое предлагал привезти на встречу, рассказывая при этом о наступающем эффекте после потребления. Таким образом, суд установил, что обвиняемый совершил склонение к потреблению наркотического средства, а именно – умышленные действия, направленные на возбуждение у потерпевший желания его потребить, действовал при этом не только с целью добиться встречи с потерпевшей, но и принудить ее к потреблению наркотического средства. Тот факт, что в дальнейшем потерпевшая выразила согласие и желание

потребить наркотическое средство, о чем она сообщила в переписке, подтверждает наличие в действиях обвиняемого состава преступления, предусмотренного п. «д» ч. 2 ст. 230 УК РФ [5].

Важную роль в установлении факта склонения к употреблению наркотических средств играют показания свидетелей, включая потерпевших. Свидетели могут подтвердить факт переписки, предложения употребить наркотики, а также описать обстоятельства, при которых это происходило. В приговоре Кировского районного суда г. Уфы от 13 августа 2024 г. по делу № 1-325/2024 показания потерпевшей были ключевым доказательством, подтверждающим факт склонения к употреблению наркотиков [3].

Доказательством также являются экспертные заключения, подтверждающие наличие наркотических средств в изъятых веществах. Экспертиза может подтвердить, что изъятые вещества действительно являются наркотическими средствами, и это усиливает доказательственную базу. Так, в приговоре Октябрьского районного суда г. Кирова от 31 марта 2023 г. по делу № 1-167/2023 суд использовал в качестве доказательства заключение эксперта, подтверждающее, что изъятое вещество содержало наркотическое средство мефедрон [4].

Кроме того, в качестве доказательств судами признаются результаты оперативно-разыскных мероприятий, а также показания оперативных сотрудников об обстоятельствах получения оперативной информации, ее реализации, проведении оперативно-разыскных мероприятий [5].

Доказательства, используемые по делам о склонении к потреблению наркотических средств с использованием информационно-телекоммуникационных сетей, обладают отличительными характеристиками.

Большинство доказательств, таких как электронная переписка, аудио- и видеосообщения, скриншоты, имеет цифровой характер. Для работы с ними требуется применение специальных методов их фиксации и исследования, чтобы исключить возможность фальсификации.

Многие доказательства, такие как переписка или показания свидетелей, являются косвенными. Они не всегда напрямую подтверждают факт склонения к потреблению, но в совокупности с другими доказательствами иногда признаются достаточными для установления вины.

Для фиксации и исследования цифровых доказательств используются специальные технические средства и программное обеспечение, что делает процесс доказывания более сложным и затратным.

Для подтверждения подлинности цифровых доказательств, таких как переписка или аудиосообщения, часто требуется проведение экспертизы, что увеличивает сроки расследования и судебного разбирательства.

Таким образом, проведенный анализ позволяет сделать вывод о том, что суды признают широкий спектр доказательств по делам о склонении к потреблению наркотических средств с использованием информационно-телекоммуникационных сетей. К ним относятся электронная переписка, аудио- и видеосообщения, скриншоты, показания свидетелей, заключения экспертов и результаты оперативно-разыскных мероприятий. Большая часть таких доказательств имеет цифровой характер, что объясняет необходимость применения специальных методов их фиксации и исследования. В совокупности такие доказательства позволяют судам устанавливать факт склонения к потреблению наркотических средств и выносить обоснованные приговоры.

Список библиографических ссылок

1. Уголовный кодекс Российской Федерации: принят Гос. Думой 24 мая 1996 г.: одобр. Советом Федерации 5 июня 1996 г.: ред. от 13 декабря 2024 г. // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

2. О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами: постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 (ред. от 16 мая 2017 г.) // Российская газета. 2006. 28 июня. № 137.

3. Приговор Кировского районного суда г. Уфы от 13 августа 2024 г. по делу № 1–325/2024. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Приговор Октябрьского районного суда г. Кирова от 31.03.2023 по делу № 1–167/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Апелляционное определение Самарского областного суда от 19.06.2024 по делу № 22–2546/2024 . Доступ из справ.-правовой системы «КонсультантПлюс».

Валерий Левонович Согоян,
доцент кафедры уголовного права, криминологии
и уголовного процесса
Ростовского филиала Санкт-Петербургской академии
Следственного комитета Российской Федерации,
кандидат юридических наук

ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЗАПРЕТА ОПРЕДЕЛЕННЫХ ДЕЙСТВИЙ

В апреле 2018 г. российское законодательство пополнилось новой мерой пресечения в виде запрета определенных действий. Данная мера пресечения была введена законодателем как альтернатива заключению под стражу, об этом говорилось в пояснительной записке к законопроекту [1].

По мере реализации требований ст. 105.1 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) появились и проблемы.

Порой следователи, возбуждая перед судом ходатайство об избрании указанной меры пресечения, предлагают установить запрет, не предусмотренный ст. 105.1 УПК РФ, а суд впоследствии переносит это незаконное требование в выносимое постановление.

Например, Верховный Суд Республики Крым апелляционным постановлением от 24 декабря 2021 г. изменил решение Алуштинского городского суда от 8 декабря 2021 г. об изменении обвиняемому меры пресечения с домашнего ареста на запрет определенных действий. В апелляционном постановлении указано: «… принимая обжалуемое решение, суд вышел за пределы уголовно-процессуального кодекса, установив запрет, не предусмотренный ст. 105.1 данного кодекса, – являться по вызовам следователя и суда, что также противоречит разумности и препятствует производству предварительного следствия по уголовному делу с участием обвиняемого, а также ставит стороны в положение, исключающее возможность исполнения постановления суда» [2].

В соответствии с требованиями ч. 11 ст. 105.1 УПК РФ осуществление контроля за соблюдением установленных запретов судами возлагается на уголовно-исполнительные инспекции ФСИН России, уполномоченные сотрудники которых посещают обвиняемых по месту их жительства, используют соответствующие технические средства, перечень и порядок применения которых определен постановлением Правительства Российской Федерации от 18 февраля 2013 г. № 134, направляют необходимые запросы в органы и учреждения.

При этом следует отметить, что в распоряжении уголовно-исполнительных инспекций ФСИН России (далее – инспекция) технические средства контроля позволяют отслеживать только выход лица за пределы жилого помещения. С их помощью практически невозможно идентифицировать лиц, с которыми запрещено общаться, точно определить расстояние до объекта, к которому запрещено приближаться, действенно контролировать использование средств связи и сети Интернет.

Также недостаточна численность сотрудников, контролирующих исполнение меры пресечения.

В описанных условиях результативность данной меры пресечения зависит в основном от добросовестности лица, к которому она применяется, что значительно

снижает превентивный потенциал новых законоположений, делая их фактически невостребованными со стороны следственных работников.

Не всегда удается достичь эффективного взаимодействия органа предварительного следствия, суда и контролирующего органа, каковым в данном случае является инспекция.

Как известно, следователь начинает взаимодействовать с инспекцией еще до избрания судом рассматриваемой меры пресечения, информируя инспекцию о возбуждении перед судом ходатайства о применении меры пресечения в виде запрета определенных действий и предстоящем судебном заседании. Такое правило содержится в п. 4 «Порядка осуществления контроля за нахождением подозреваемых или обвиняемых в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением возложенных судом запретов подозреваемыми или обвиняемыми, в отношении которых в качестве меры пресечения избран запрет определенных действий, домашний арест или залог» (далее – порядок осуществления контроля) [3].

Одна из проблем оперативного взаимодействия заключается в том, что инициатива избрания данной меры пресечения может принадлежать суду. Так, согласно ч. 7.1 ст. 108 УПК РФ, суд, отказывая в удовлетворении ходатайства об избрании меры пресечения в виде заключения под стражу, может по собственной инициативе избрать иную меру пресечения, в частности, в виде запрета определенных действий. В результате инспекция оказывается своевременно не уведомлена, а следователь – не подготовлен к реализации данной меры пресечения.

Во избежание подобных ситуаций требуется производить все возможные следственные и иные действия как по сбору характеризующих сведений, так и по выяснению данных, свидетельствующих о наличии оснований и обстоятельств, указанных в ст. 97 и 99 УПК РФ.

Руководством Следственного комитета Российской Федерации для обеспечения эффективного контроля за лицами, в отношении которых избрана мера пресечения в виде запрета определенных действий, до принятия уполномоченным органом необходимых нормативных правовых актов рекомендуется следственным органам непосредственно после вынесения соответствующего судебного решения организовывать надлежащее взаимодействие с контролирующим органом и с органами полиции – с учетом их компетенции. Одним из способов повышения результативности межведомственного взаимодействия в рассматриваемой сфере может быть заключение соответствующих соглашений с региональными управлениями ФСИН России.

Гипотетическим видится и указание данных, позволяющих идентифицировать лиц, с которыми подозреваемому (обвиняемому) запрещено общение, – как это указано в п. 40 постановления Пленума Верховного Суда РФ от 19 декабря 2013 г. № 41 (ред. от 11 июня 2020 г.) «О практике применения судами законодательства о мерах пресечения в виде заключения под стражу, домашнего ареста, залога и запрета определенных действий» [4].

Запрет в виде общения с определенными лицами зачастую трактуется судами достаточно широко, что также не способствует оперативному взаимодействию следователя с контролирующими лицами (органами).

И если указание о невозможности общения со всеми лицами, кроме близких родственников и защитников [5], без письменного разрешения следователя не представляет особой сложности в реализации меры пресечения, то указание в постановлении запрета «общаться с лицами, являющимися по уголовному делу свидетелями, потерпевшими, обвиняемыми или подозреваемыми» [6] вызывает определенные затруднения. Судом в этом случае используется формулировка, не позволяющая

в полной мере идентифицировать круг этих лиц. Также отметим, что в справке по уголовному делу, направляемой в инспекцию, прямо предусмотрено указание контактных данных защитника, а в п. 6 порядка осуществления контроля – необходимость предоставления изменений в этих сведениях в течение 24 часов. О свидетелях
и других фигурантах уголовного дела в порядке осуществления контроля ничего не сказано [3]. Конечно, эти сведения можно отнести к информации о совершенном преступлении. Но ведь круг свидетелей в процессе расследования изменяется, и это приводит к необходимости постоянного обновления информации о лицах, с которыми запрещено общение.

В порядке осуществления контроля предусмотрены действия инспекции при установлении факта нарушения подозреваемым (обвиняемым) запрета определенных действий, включающие информирование следователя. В то же время порядок осуществления контроля не регулирует информирование следователем инспекции, когда ему становится известно о таких нарушениях, к примеру, из показаний свидетелей, потерпевших.

Список библиографических ссылок

1. Пояснительная записка к проекту Федерального закона «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации (в части избрания и применения мер пресечения в виде залога, запрета определенных действий и домашнего ареста)». URL: http://base.garant.ru/57722915/ (дата обращения: 30.01.2025).

2. Дело № 22К-3819/2021 // Судебные решения РФ: офиц. сайт. URL: https://судебныерешения.рф/65093383 (дата обращения: 30.01.2025).

3. Об утверждении Порядка осуществления контроля за нахождением подозреваемых или обвиняемых в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением возложенных судом запретов подозреваемыми или обвиняемыми, в отношении которых в качестве меры пресечения избран запрет определенных действий, домашний арест или залог: приказ Министерства юстиции Российской Федерации, МВД России, Следственного комитета Российской Федерации и ФСБ России от 31 августа 2020 г. № 189/603/87/371 (зарегистрировано в Минюсте России 3 сентября 2020 г. № 59635). URL: https://legalacts.ru/doc/prikaz-miniusta-rossii-n-189-mvd-rossii-n-603/ (дата обращения: 30.03.2025).

4. О практике применения судами законодательства о мерах пресечения в виде заключения под стражу, домашнего ареста, залога и запрета определенных действий: постановление Пленума Верховного Суда Российской Федерации от 19 декабря 2013 г. № 41 (ред. от 11 июня 2020 г.) // Верховный Суд Российской Федерации: офиц. сайт. URL: https://www.vsrf.ru/documents/own/8379/ (дата обращения: 15.03.2025).

5. Апелляционное постановление Московского городского суда от 16 декабря 2020 г. № 10-189662/2020. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Апелляционное постановление Московского городского суда от 7 сентября 2020 г. по делу № 10-16580/2020. Доступ из справ.-правовой системы «КонсультантПлюс».

***Денис Валентинович Теткин*,**
доцент кафедры уголовного процесса Рязанского филиала
Московского университета МВД России имени В. Я. Кикотя,
кандидат юридических наук

ОСОБЕННОСТИ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В эпоху цифровизации количество преступлений, совершаемых с использованием сети Интернет и информационно-телекоммуникационных технологий (далее – ИТТ), растет с геометрической прогрессией, и это проявляется в различных сферах жизнедеятельности людей. Преступления рассматриваемой категории зачастую не имеют территориальных границ ввиду использования виртуального киберпространства. Они могут совершаться одновременно в нескольких территориальных единицах, в международном интернет-пространстве и затрагивать интересы пострадавших, находящихся в нескольких странах.

Цифровизация большинства сфер жизни, денежных потоков, а также различных действий, необходимых для жизнеобеспечения (запись к врачу, оформление кредитов через онлайн-приложения банков, покупки в онлайн-магазинах и т. д.), и перенос персональных данных в базы данных различных сервисов дают современным преступникам доступ к огромному объему информации, касающейся простых граждан. Эта информация может быть использована для совершения преступлений. Уязвимыми оказываются организации и предприниматели, если преступники получают доступ к информации о деятельности в сфере бизнеса.

В связи с тем, что имеющие свою специфику преступления, совершаемые с использованием интернет-технологий, ввиду новизны только начинают исследоваться учеными, вопросы разработки тактики и методов расследования данных видов преступлений приобрели огромную актуальность.

Расследование таких преступлений относится к категории не самых простых дел. Чаще всего возбужденное уголовное дело не доходит до судебного разбирательства в связи с отсутствием лица, подлежащего привлечению к уголовной ответственности [1]. Требует решения вопрос подготовки профессиональных кадров, способных выявлять, расследовать и доказывать факты подобных преступлений.

Алгоритм расследования преступлений с использованием интернет-технологий складывается из первоначальной следственной ситуации и наличия определенных признаков состава преступления. Расследование имеет ряд особенностей. Принимая решение о возбуждении уголовного дела, следователь должен понимать и знать, какие обстоятельства ему предстоит установить и доказать в ходе расследования. Необходимо также понимать, каких специалистов, обладающих компетенциями в области применения компьютерных технологий, стоит привлечь для содействия в доказывании обстоятельств уголовного дела.

Можно выделить несколько типов следственных ситуаций, складывающихся на первоначальном этапе расследования преступлений, совершенных с использованием интернет-технологий:

1. Отсутствие информации о мотивах, способе совершения и личности преступника.

2. Отсутствие информации о личности преступника при наличии информации о способе совершения преступления и мотиве.

3. Известны способы совершения и сокрытия преступления, а также личность преступника и другие обстоятельства преступления [2].

Исходя из первоначальной следственной ситуации, которая может постоянно обновляться и меняться под воздействием различных факторов, разрабатываются новые версии и план следующего этапа расследования.

Возбуждению уголовного дела по данной категории преступлений всегда предшествует предварительная проверка документов и фактов, основываясь на результатах которой следователь может выбрать оптимальную предварительную последовательность первоначальных следственных действий, организационных мероприятий. Эффективность его работы зависит от оперативности реагирования на сообщение о совершенном преступлении: запоздалое принятие решения о возбуждении уголовного дела может привести к утрате доказательств, увеличению сроков предварительного расследования и другим негативным последствиям.

При производстве первоначальных следственных действий важную роль играют установление мотива и лиц, виновных в преступлении, возможность задержания преступника, вызов необходимых специалистов для участия в осмотре места происшествия, а также установление места преступления.

Назовем основные первоначальные следственные действия по данной категории преступлений.

1. Осмотр места происшествия с привлечением необходимых специалистов, компетентных в сфере ИТТ.

Осмотр места происшествия при расследовании дел рассматриваемой категории является важным следственным действием, направленным на обнаружение следов преступления и установление иных обстоятельств, имеющих значение для уголовного дела. При этом осмотр места происшествия имеет свои особенности, связанные как с характером самих преступлений, так и со спецификой устройств и данных, которые использовались для его совершения или на которые были направлены преступные действия. К таким особенностям можно отнести

– участие специалиста, обладающего специальными знаниями в сфере информационно-телекоммуникационных технологий, способного в ходе осмотра места происшествия использовать специализированное оборудование и программы, позволяющие восстановить удаленные данные или провести анализ логов;

– проведение идентификации источника данных (необходимо учитывать, что объектом осмотра места происшествия могут быть как физические устройства, так и облачные сервисы). Осмотру подлежат и локальные устройства, и сетевые ресурсы (например, маршрутизаторы, серверы, персональные компьютеры, находящиеся в одной локальной сети), предоставляющие возможность проведения анализа трафика;

– акцентирование внимания на сборе цифровых улик – данных, хранящихся на устройствах, логов доступа, переписок и др.;

– проведение анализа социальных сетей, исследование активности и взаимодействия, связанных с ними (если преступление совершено с использованием указанных ресурсов);

– изъятие всех источников информации в ситуации, при которой извлечение данных из упомянутых источников может привести к их утрате.

2. Осмотр места преступления (при его установлении). По данной категории дел установить место преступления очень проблематично, поскольку оно всегда

дистанцировано от места происшествия. В случае его установления важно учитывать особенности, характерные для осмотра места происшествия, и не упускать из виду уже имеющиеся факты и обстоятельства.

3. Обыски подозреваемых (личные, мест проживания, рабочих мест). Первостепенной задачей обыска является изъятие предметов, которые могли использоваться в качестве орудий преступлений и хранить доказательства преступной деятельности.

Обыск проводится с целью изъятия персональных компьютеров, мобильных телефонов, жестких дисков, а также иных запоминающих устройств. Важным моментом является привлечение специалиста, без которого изъятие электронных носителей информации не допускается. Возможность копировать данные, хранящиеся на запоминающем устройстве, предоставляется по ходатайству законного владельца или обладателя информации. При этом следователь вправе отказать в удовлетворении ходатайства, если процесс копирования способен повлечь утрату или изменение хранящейся на носителе информации. Следователь также вправе осуществлять копирование информации, при этом важно правильно процессуально закрепить это действие. В протоколе должны быть указаны технические средства, применявшиеся для копирования, порядок их применения, запоминающие устройства, на которые осуществляется перенос данных, и результаты выполненных действий. В последующем электронные носители прилагаются к протоколу.

4. Допросы потерпевших, свидетелей, подозреваемых лиц.

Именно допрос потерпевшего позволяет получить наиболее полное представление об обстоятельствах преступления и механизме его совершения. Не стоит подходить к допросу потерпевшего формально, поскольку его показания могут содержать информацию, еще неизвестную для следствия. Проведение допроса осуществляется в два этапа: подготовка, в ходе которой следователь изучает материалы дела и на основании имеющихся данных составляет список вопросов, и проведение допроса, в ходе которого следователь выявляет максимальный объем информации, значимой для уголовного дела, чтобы впоследствии, при проведении анализа, использовать ее наиболее эффективно в ходе расследования.

Проведение допроса свидетелей и подозреваемых по данной категории дел не всегда представляется возможным ввиду характера данных преступлений. Если же такие лица установлены, то следователю необходимо создать благоприятную следственную ситуацию, чтобы получить от допрашиваемых наиболее полную и достоверную информацию.

5. Проведение следственного эксперимента.

Это действие становится возможным в том случае, если есть лицо, совершившее преступление, и оно готово способствовать расследованию. В ходе следственного эксперимента могут быть проверены навыки его участника по использованию тех или иных устройств, а также выявлена последовательность происшедшего события.

6. Анализ полученной информации, документации, принятие решений о проведении экспертиз.

Перечень экспертиз, назначаемых по данным преступлениям, достаточно широк. Необходимость проведения каждой конкретной экспертизы определяется способом совершения преступления, орудием совершения преступления и объектом преступного посягательства. Наиболее часто проводятся компьютерно-техническая, бухгалтерская и психиатрическая (в отношении потерпевших) экспертизы.

Для получения информации следователь должен использовать широкий набор инструментов и иметь доступ к определенным данным, получение которых осуществляется в результате формирования различных видов запросов, направляемых интернет-провайдерам, – об IP-адресах, о принадлежности реквизитов доступа к Интернету, реквизитах электронной почты, регистрации имен доменов, регистрации в электронных платежных системах, – и других, позволяющих подтвердить причастность злоумышленников к совершенному преступлению.

В ходе следствия в банки направляются запросы о предоставлении информации (выясняются анкетные данные владельцев счета, место поступления денежных средств пострадавшего лица (лиц), движения денежных средств). Для получения таких сведений, чаще всего относимых к охраняемой законом тайне, необходима санкция суда. Следователи готовят материалы для ходатайства по запросу в каждую организацию. Запросы очень часто долго обрабатываются банками и другими организациями, нередко требуется отправка повторных запросов. Это затрудняет своевременное проведение оперативно-разыскных мероприятий и выявление лиц, ответственных за совершенные преступления.

Завершая описание результатов исследования проблемного вопроса, касающегося особенностей следственных действий на первоначальном этапе расследования преступлений с использованием интернет-технологий, отметим следующее: представленные позиции могут изменяться в процессе совершенствования следственной практики и развития у сотрудников органов внутренних дел, занимающихся расследованием преступлений рассматриваемой категории, профессиональных компетенций в области цифровизации.

Список библиографических ссылок

1. Лаврушкина А. А. Типичные следственные действия в рамках методики расследования мошенничества с использованием сети Интернет и средств мобильной связи // Бюллетень науки и практики. 2018. Т. 4. № 4. С. 447–451. URL: http://www.bulletennauki.com/lavrushkina-a (дата обращения: 30.01.2025).

2. Олиндер Н. В. Следственные действия на первоначальном этапе расследования преступлений, совершенных с использованием электронных платежных средств и систем // Юридический вестник СамГУ. 2015. Т. 1. № 4. С. 87–91. URL: https://journals.ssau.ru/jjsu/issue/view (дата обращения: 30.01.2025).

Екатерина Андреевна Хазинурова,
адъюнкт адъюнктуры
Санкт-Петербургского университета МВД России

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ БОРЬБЫ С ИСПОЛЬЗОВАНИЕМ DEEPFAKE-ТЕХНОЛОГИЙ В ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ

С развитием технологий искусственного интеллекта (далее – ИИ) и машинного обучения появились новые способы обработки цифровых ресурсов, которые могут быть использованы как в легальных, так и в преступных целях. К таким технологиям относится deepfake – метод создания с помощью ИИ поддельных изображений, аудио- и видеозаписей, практически неотличимых от реальных.

Deepfake (от англ. deep learning – глубокое обучение и fake – подделка) – технология, основанная на использовании нейронных сетей для создания изображений, аудио и видео.

Термин стал популярным в 2017 г., когда пользователь Reddit под ником deepfakes начал выкладывать поддельные видео с заменой лиц знаменитостей [1].

Основными этапами создания deepfake являются

– сбор и обработка исходных данных (фото, видео, аудио);

– обучение нейронной сети на основе этих данных;

– генерация нового контента, имитирующего реальные объекты.

Deepfake-технологии активно применяются киберпреступниками, например, при осуществлении ими мошенничества с использованием информационно-телекоммуникационных технологий, кражи персональных данных, вымогательства в социальных сетях, фишинга и других противоправных деяний.

Уголовно-правовые аспекты борьбы с использованием deepfake-технологий в первую очередь требуют совершенствования норм законодательства, разработки технико-криминалистических методов выявления подобных преступлений и повышения уровня подготовки сотрудников органов внутренних дел в области информационных технологий.

Технология deepfake имеет широкий спектр применения – кино, реклама и маркетинг, образование и игры. В качестве же инструмента для совершения преступлений она представляет серьезную угрозу. Использование deepfake-технологий в преступной деятельности квалифицируется по различным статьям Уголовного кодекса Российской Федерации (далее – УК РФ) в зависимости от целей преступления и его последствий [2]. К основным видам противоправных деяний, связанных с применением deepfake-технологий, относятся

– мошенничество (ст. 159 УК РФ) – использование поддельных аудио- и видеозаписей с целью получения материальной выгоды;

– клевета (ст. 128.1 УК РФ) – распространение ложной информации с использованием deepfake-технологий, подрывающей репутацию лица;

– вымогательство (ст. 163 УК РФ) – создание компрометирующих материалов для шантажа;

– незаконные изготовление и оборот порнографических материалов или предметов (ст. 242 УК РФ) и изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ) – создание поддельных изображений или видео сексуального характера для демонстрации или

рекламирования с использованием средств массовой информации (далее – СМИ) либо информационно-телекоммуникационных сетей, в том числе сети Интернет;

– терроризм (ст. 205 УК РФ) – использование deepfake-технологий для распространения в СМИ и социальных сетях ложных сообщений о террористических актах.

Однако действующее уголовное законодательство не всегда учитывает специфику современных технологий, вследствие чего возникают пробелы в правовом регулировании. Введение самостоятельной уголовной ответственности за создание и распространение deepfake может столкнуться с существенными сложностями в части квалификации подобных деяний. Основная проблема заключается в том, что названные действия часто будут требовать дополнительной квалификации по другим статьям УК РФ, связанным с преступлениями, совершенными с использованием deepfake (например, ст. 128.1, 242.1 УК РФ и др.), что приведет к утрате значимости нового самостоятельного состава преступления, возникновению ситуации двойного учета одного и того же деяния [3, с. 80]. В результате может произойти неоправданное ужесточение уголовной ответственности, противоречащее принципам справедливости и соразмерности наказания.

Необходимо тщательно проработать механизмы квалификации преступлений, совершенных с применением технологии deepfake, чтобы избежать дублирования норм и обеспечить баланс между защитой общественных интересов и соблюдением прав личности. Именно поэтому поиск оптимального баланса в правовом регулировании распространения информации в сети Интернет, а также разработка эффективного комплекса мер для противодействия фальшивым новостям остаются ключевыми задачами для правовых систем большинства современных государств и крупных социальных онлайн-платформ [4, с. 15].

Выявление и расследование преступлений, связанных с использованием deepfake-технологии, требует применения следующих технико-криминалистических методов:

– анализ цифровых данных (использование специализированного программного обеспечения для обнаружения следов редактирования и генерации контента);

– исследование электронных ресурсов (проведение экспертизы для установления подлинности аудио, видео и изображений);

– использование блокчейн-технологий (верификация источников информации и предотвращение распространения подделок);

– разработка алгоритмов машинного обучения (автоматическое обнаружение deepfake-контента).

Особое значение имеет подготовка специалистов в области цифровой криминалистики, способных эффективно работать с современными технологиями.

В настоящее время в МВД используется программа «Зеркало» (или «Верблюд»), способная распознавать видео с подмененными лицами [5].

Для эффективного противодействия преступлениям, совершаемым с применением технологии deepfake, необходимо внести изменения в законодательство. Предлагаемые меры включают:

1. Ужесточение уголовного наказания за использование deepfake-технологии в террористической деятельности и при распространении порнографических материалов.

2. Разработку международных стандартов и соглашений между государствами для борьбы с трансграничными преступлениями, связанными с применением deepfake-технологии.

Использование технологии deepfake в преступной деятельности представляет серьезную угрозу для общества и требует комплексного подхода при организации противодействия подобным преступлениям. Совершенствование уголовного законодательства, развитие технико-криминалистических методов и повышение квалификации сотрудников правоохранительных органов – ключевые направления этого противодействия.

Список библиографических ссылок

1. Панасенко А. Технологии Deepfake как угроза информационной безопасности. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Deepfakes-as-a-information-security-threat (дата обращения: 06.03.2025).

2. Уголовный кодекс Российской Федерации: принят Государственной Думой 24 мая 1996 г.: одобр. Советом Федерации 5 июня 1996 г.: ред. от 13 декабря 2024 г. // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 3397.

3. Ситник В. Н. Перспективы установления уголовной ответственности за преступления, совершенные с использованием технологии дипфейк // Уральский журнал правовых исследований. 2022. № 3. С. 76–83.

4. Алферова Е. В., Иванова А. П. Правовое регулирование в сфере борьбы с дезинформацией в сети Интернет // Правовая информатика. 2023. № 3. С. 11–17.

5. Хохлов А. А., Лыкова А. Б., Никонорова Л. И. Дипфейк и общественная безопасность // Наука и Образование. 2024. Т. 7. № 2. URL: http://opusmgau.ru/index.php/see/article/view/6787/6849 (дата обращения: 15.04.2025).

РАЗДЕЛ II.
МОЯ ПРОФЕССИЯ – СЛЕДОВАТЕЛЬ

(Всероссийская научно-практическая конференция,
посвященная 62-й годовщине образования органов предварительного следствия
в системе МВД России, Волгоградская академия МВД России,
г. Волгоград, 4 апреля 2025 г.)

Роман Рифович Абсатаров,
старший преподаватель кафедры криминалистики
Калининградского филиала
Санкт-Петербургского университета МВД России,
кандидат географических наук

ИСПОЛЬЗОВАНИЕ КОГНИТИВНОГО ПОДХОДА ПРИ ПРОИЗВОДСТВЕ ДОПРОСА УЧАСТНИКОВ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Показания потерпевших и свидетелей играют значительную роль в уголовном процессе, поскольку они могут существенно влиять на результаты расследования дела. Обычно эти показания – один из основных источников информации о преступлении и имеют самостоятельное значение в системе доказательств. При расследовании преступлений часто возникают ситуации, когда лицо, бывшее в прошлом свидетелем определенного события или имеющее важные сведения, в процессе следственных действий оказывается неспособным восстановить информацию из-за естественного забывания или потери памяти, вызванной стрессом или травмой. Именно поэтому следователю необходимо обладать определенными навыками и умениями в общении, а также понимать принципы работы мозга, связанные с памятью [1, с. 17–19].

В настоящее время в практике правоохранительных органов все большее распространение получает метод когнитивного интервью. В основе техники опроса, проводимого с использованием когнитивных методик, лежат знания о закономерностях функционирования познавательных процессов человека.

Существует мнение, что человек помнит все из своей жизни полностью с момента рождения, но без определенной методики восстановить ясно в памяти не может. Одними из первых, кто внедрил специальные методы когнитивного интервью, были известные американские психологи Э. Гейзельман и Р. Фишер.

После многих лет клинических исследований ученые пришли к выводу о необходимости внедрения метода когнитивного интервью в криминалистическую тактику проведения допроса.

Когнитивное интервью – это специальный метод допроса, позволяющий допрашиваемому вспомнить информацию о внешности преступника, его поведении и обстоятельствах преступления.

К основным приемам, используемым при проведении когнитивного интервью, следует отнести

– мысленное воссоздание события;

– вербальное воссоздание события и контекста;

– детализацию;

– припоминание обстоятельств в различной последовательности;

– смену перспективы.

Допрашиваемому предлагается как можно более подробно описать происшествие безотносительно к самому факту преступления. При этом порядок событий также может быть любым.

Приемы, связанные с особенностями запоминания информации, – мнемотехнические – направлены на восстановление в памяти не только самого события, но и фона, контекста, в котором оно совершилось. Например, допрашиваемому лицу предлагается вспомнить, какое настроение у него было в день происшествия, какая стояла погода, какие переживания возникли у индивида, когда он непосредственно столкнулся с преступлением.

При проведении когнитивного интервью могут быть использованы дополнительные приемы, способствующие активизации памяти. Например, свидетелю или потерпевшему задаются вопросы о том, напоминал ли преступник кого-то из тех, кто хорошо знаком допрашиваемому; упоминал ли преступник какие-то необычные слова, выражения и т. п.

Следует отметить, что данный метод в нашей стране стал использоваться относительно недавно. Первое применение в следственной практике страны относится к 1992 г. [2, с. 64–68].

Основным ограничением применения когнитивного интервью как способа активизации памяти является неготовность допрашиваемого лица к сотрудничеству. По этой причине данный метод используется при допросе потерпевших и свидетелей, но его применение в отношении подозреваемых может быть неэффективным.

В проведении когнитивного интервью выделяются несколько этапов:

– установление психологического контакта;

– объяснение цели интервью;

– свободный рассказ;

– направленные вопросы;

– расширенный поиск;

– краткий обзор;

– завершающая стадия [3, с. 47–52].

Рассмотрим данные этапы подробно.

Залогом эффективности проведения когнитивного интервью является создание спокойной доверительной обстановки и установление психологического контакта. Важно расположить допрашиваемого к общению со специалистом и следователем. Специалист должен обратить внимание допрашиваемого на определенные условия взаимодействия:

– максимально сконцентрироваться, усиленно работать;

– ничего не пропускать;

– не придумывать ответы.

На этапе свободного рассказа допрашиваемому предлагается описать события, предварявшие происшествие, но непосредственно с ним не связанные (например, куда шел, что собирался делать, как себя чувствовал, какая была погода, кого встретил, с кем говорил по телефону и т. д. перед тем, как совершилось преступление). Затем предлагается в свободной форме изложить события самого преступления, очевидцем которого стал допрашиваемый. Свидетель описывает обстановку места происшествия, объекты, которые там были расположены, дает их визуальные характеристики.

Можно предложить очевидцу изменить последовательность припоминания. Как правило, интервьюируемые начинают рассказ, обращаясь к эпизодам, наиболее удаленным во времени от события преступления, в той же последовательности, в какой сменялись действия. Существует вероятность того, что, описывая события в обратном порядке, свидетель сможет вспомнить гораздо больше деталей. Допустимо и использование приема, получившего название «смена перспективы»: допрашиваемому предлагается описать события, посмотрев на них глазами другого участника, очевидцев произошедшего.

Специалист, оценив полученную информацию, определяет дальнейшую стратегию и намечает последовательность вопросов, которые необходимо задать свидетелю, чтобы полностью восстановить картину случившегося.

Расширение объема точной информации становится возможным при использовании техники мысленного представления деталей события. С этой целью психолог может предложить допрашиваемому конкретизировать образы, всплывающие в его памяти. Например, при составлении субъективного портрета преступника специалист-психолог формулирует для свидетеля такие задачи: как можно яснее перед своим мысленным взором представьте этого человека; представьте его внешний вид – и задает вопросы следующего характера: во что был одет преступник? что бы Вы могли сказать о его запахе? что он сказал?

Большое значение в процессе расследования имеет выяснение фамилий и имен, употребленных в разговоре участников исследуемого события. При затруднении в ответах допрашиваемому может быть предложено путем перебора алфавита восстановить, было ли упомянутое имя (фамилия) иностранным; вспомнить, не обменивались ли участники события словами, называющими количество, числа, цифры; уточнить, какие особенности имели голоса (наличие акцента у действующих лиц, их интонации и речевые характеристики) [4, с. 62–67].

Цель направленных вопросов – индивидуализация объектов, лиц, устанавливаемых по данному уголовному делу. В памяти интервьюируемого содержится некий «набор характеристик» события, образующих своеобразную «цепочку». Например, свидетель помнит, что к одному из участвовавших в совершении преступления обратились по имени (кличке), но затрудняется конкретизировать. Можно попросить интервьюируемого припомнить, было ли это имя длинным или коротким, какие ассоциации, эмоции оно вызвало. В итоге комбинация таких «цепочек» может привести к восстановлению деталей, интересующих следствие.

Подводя итог, отметим, что когнитивное интервью на сегодняшний день является одним из наиболее эффективных методов активизации памяти потерпевших и свидетелей. Большое значение имеет готовность свидетеля к сотрудничеству, его желание помочь следствию. Он в обязательном порядке должен быть очевидцем события, непосредственным наблюдателем.

Список библиографических источников

1. Абсатаров Р. Р. Психологический реагент и его криминалистическое значение // Криминалистическая тактика: история, современное состояние и перспективы развития (к 85-летию со дня рождения профессора В. И. Комиссарова): материалы Междунар. науч.-практ. конф., Москва, 14 марта 2024 г. М.: Проспект, 2024. С. 17–19.

2. Панькина И. Ю., Трофимова Т. В. Когнитивное интервью при допросе на предварительном расследовании // Допустимость показаний в уголовном процессе: сборник статей по материалам Всероссийского круглого стола, Санкт-Петербург,

19 декабря 2020 г. СПб.: Центр научно-информационных технологий «Астерион», 2021. С. 64–68.

3. Ерахтина Е. А. Когнитивная психология в методах допроса свидетеля // Обеспечение прав участников уголовного судопроизводства с ограниченными возможностями: компенсаторный подход: материалы Междунар. науч.-практ. конф., Красноярск, 18–19 июня 2021 г. Часть 2. Красноярск: Красноярский государственный аграрный университет, 2021. С. 47–52.

4. Болатханова К. Р. Актуальные проблемы когнитивной психологии при проведении допроса // European Science. 2016. № 12 (22). С. 62–67.

Ольга Павловна Виноградова,
доцент кафедры криминалистики
Уральского юридического института МВД России,
кандидат юридических наук, доцент

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ КРИМИНАЛИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

В современном обществе отмечаются высокие темпы цифровизации различных отраслей деятельности. Одним из интересных и перспективных направлений цифровизации общества является развитие технологии искусственного интеллекта. Согласно положениям указа Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека[1].

В научном сообществе давно ведется дискуссия относительно понятия искусственного интеллекта. Так, при анализе научных статей и исследований смежной тематики отмечается, что нередко данное понятие получает более широкое толкование в сравнении с тем, что процитировано выше. Например, по мнению Э. А. Абдуллаева, искусственный интеллект – часть сферы информационно-коммуникационных технологий, представленная аппаратно-программными комплексами, близкими по своим аналитическим способностям к способностям человеческого мозга [1]. Также необходимо отметить, что теории искусственного интеллекта включают в себя ряд узконаправленных технологических разделов, которые в совокупности позволяют реализовывать функции искусственного интеллекта. К данным разделам относятся, например, нейронные сети, глубокий анализ данных, машинное обучение и др.

В настоящее время все возрастает количество людей, выражающих уверенность в том, что будущее человечества – за искусственным интеллектом. Так, в США функционирует объединенный центр искусственного интеллекта Министерства обороны. Во Франции открыт Национальный институт исследований в области цифровых наук и технологий Inria. Многие страны (Эстония, Сингапур, Франция, Канада, Саудовская Аравия и другие) разрабатывают свои национальные стратегии в области искусственного интеллекта [2]. Эти данные свидетельствуют о глубокой заинтересованности большинства развитых государств в совершенствовании технологии, которая уже применяется во многих сферах жизни общества: в экономике, бизнесе, производстве, медицине, правоохранительной деятельности.

Интересно отметить использование технологии в оперативно-разыскной деятельности. Так, для сотрудников, правомочных осуществлять эту деятельность, искусственный интеллект может стать незаменимым помощником при сборе информации и розыске преступников. Уже сегодня он внедряется в работу различных систем

[1] О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10 октября 2019 г. № 490 // Официальный интернет-портал правовой информации. Государственная система правовой информации: сайт. URL: http//pravo.gov.ru (дата обращения: 27.02.2025).

безопасности. Например, система «Безопасный город» позволяет определять личность человека по его внешности. Система пока не лишена недостатков: для совершенствования необходимо обеспечить ее возможностью выполнения функции идентификации транспортных средств, а также распространить ее применение на камеры, установленные в домофонах жилых домов, банкоматах, магазинах и иных комкоммерческих учреждениях.

Использование технологии искусственного интеллекта в деятельности органов предварительного следствия давно стало предметом научной дискуссии в связи с тем, что, по мнению ученых, искусственный интеллект не способен учитывать ряд существенных обстоятельств. Таким образом, в контексте процессуальной деятельности технологию следует рассматривать как помощника при планировании следственных действий, заполнении документов, сборе недостающей информации, сопоставлении фактов (в целях выявления лжи, например, при допросе) и др.

Вопрос внедрения системы искусственного интеллекта в деятельность экспертных подразделений МВД России – один из наиболее противоречивых. С одной стороны, эта деятельность предполагает выполнение ряда унифицированных процедур, которые искусственный интеллект выполнить способен, однако требования, предъявляемые к производству экспертиз, исключают возможность применения данных технологий в судебно-экспертной деятельности (часто результаты искусственного интеллекта не раскрывают методологии, полученных результатов). Так, представляется целесообразным в качестве эксперимента внедрить системы искусственного интеллекта в судебно-экспертную деятельность. При этом на начальном этапе технология должна выполнять исключительно подсобные функции (анализ данных, информирование эксперта о выявленных признаках, классификация данных, учет и автоматизация банков данных). В дальнейшем – по мере развития технологии – представляется перспективным полноценное внедрение искусственного интеллекта в процесс производства экспертиз. Один из предполагаемых шагов на пути к достижению этой цели – возможность указания искусственному интеллекту на производство исследования с учетом определенной методологии.

Следует сказать, что судебно-экспертная деятельность требует наличия глубоких познаний, навыков осуществления исследований.

В настоящее время в судебно-экспертной деятельности широко применяются различного рода достижения науки и техники. Заслуживает внимания производство компьютерных экспертиз, среди которых выделяются аппаратно-программная экспертиза, программно-компьютерная экспертиза, информационно-компьютерная экспертиза и компьютерно-сетевая экспертиза.

Таким образом, современная технология может использоваться в экспертной деятельности и как объект исследования, и как вспомогательный (или даже основной) инструмент при производстве экспертизы.

Внедрение в судебно-экспертную деятельность и использование в ней компьютерных технологий, математических моделей свидетельствует о том, что система искусственного интеллекта в будущем найдет в ней закономерное применение. На данный момент в судебно-экспертной деятельности уже функционируют системы слабого искусственного интеллекта.

Некоторые специалисты относятся к перспективам внедрения систем развитого искусственного интеллекта в судебно-экспертную деятельность скептически, но есть и другое мнение, высказываемое учеными. Так, А. И. Хмыз, рассматривающий возможность использования ЭВМ при экспертном анализе почерка, утверждает, что в настоящее время работа систем искусственного интеллекта не дает разъяснения

конкретно применяемой методологии в процессе исследования, соответственно, говорить о достоверности представленных сведений тяжело [3]. В. А. Макаров отмечает, что роль технологии искусственного интеллекта в судебно-экспертном деле при исследовании вещественных доказательств, в основном, должна быть ориентирующей или вспомогательной, то есть сводиться либо к осуществлению информационно-аналитического обеспечения банками данных, либо к идентификации определенных признаков, которые в настоящее время с высокой степенью точности могут быть выявлены системой искусственного интеллекта [2].

Необходимо отметить, что искусственный интеллект способен к простому анализу и самообучению (накоплению и расширению информации). Таким образом, представляется целесообразным внедрение систем искусственного интеллекта в криминалистическую технику: они смогут вести криминалистический учет, производить некоторые простейшие экспертные исследования. При этом в процессе внедрения должны выполняться некоторые условия:

– заявленное внедрение систем искусственного интеллекта должно носить экспериментальный характер; необходимо анализировать и соотносить результаты работы систем искусственного интеллекта, формировать оценку эффективности их работы;

– для достижения чистоты эксперимента целесообразно локализовать его в пределах отдельной территориальной единицы Российской Федерации (например, определенного субъекта);

– результаты работы систем искусственного интеллекта могут использоваться лишь в одностороннем порядке как консультационные системы, банки данных, справочные материалы и др.; при этом система искусственного интеллекта не должна обращаться к результатам работы эксперта в целях соблюдения безопасности данных.

В ряде случаев ученые и специалисты отмечают целесообразность использования систем искусственного интеллекта в криминалистической тактике и методике. Ожидается, что искусственный интеллект сможет проанализировать практический опыт правоохранительной деятельности и выявить наиболее корректные приемы и методы раскрытия и расследования преступлений, производства экспертной деятельности, использования сил и средств и др. При этом особый интерес представляет классифицирование системами искусственного интеллекта тактики и методики раскрытия и расследования отдельных категорий преступлений. Однако, по нашему мнению, на современной стадии развития искусственного интеллекта это невозможно: пока он может анализировать, собирать, группировать и др., но не создавать что-то новое. Так, при применении в области криминалистической тактики системы искусственного интеллекта могут предложить только оптимальный тактический прием или комбинацию, исходя из типичной тактической ситуации.

Опираясь на мнения разных ученых, выражаемые по поводу внедрения искусственного интеллекта в криминалистику, отметим особо позицию Д. В. Бахтеева, размышляющего о перспективах развития технологии: «Можно обнаружить признание исследователями возможностей разработки частных методик расследования, алгоритмизации процесса расследования, повышение эффективности экспертных исследований, анализ и обобщение данных и т. д. В дополнение к выгоде внедрения искусственного интеллекта в криминалистику можно установить и наличие выгоды для развития искусственного интеллекта. Одним из качеств искусственного интеллекта является его возможность к самообучению, то есть в результате его пусть

и экспериментального внедрения искусственный интеллект сможет приобрести новые способности, что продвинет исследования в данной области вперед» [4].

В настоящее время в судебно-экспертной деятельности применяется большое количество компьютерных технологий, математических и статистических моделей. Так, в качестве следующего шага развития судебно-экспертной деятельности представляется целесообразным внедрение систем искусственного интеллекта. О полноценном внедрении говорить еще рано: на настоящий момент существует ряд вопросов, связанных с обеспечением безопасности, возможностью использования определенных результатов, полученных системами искусственного интеллекта в ходе реализации экспертно-судебной деятельности. Наиболее целесообразным видится использование системы искусственного интеллекта в судебно-экспертной деятельности в формате эксперимента.

Список библиографических источников

1. Абдуллаев Э. А. Искусственный интеллект: текущие достижения и перспективы // Молодой ученый. 2023. № 33 (480). С. 9–10.

2. Макаров В. А. Вопросы внедрения искусственного интеллекта в разделы криминалистики // Молодой ученый. 2023. № 49 (496). С. 324–326.

3. Хмыз А. И. Использование возможностей искусственного интеллекта в судебной экспертизе // Вестник экономической безопасности. 2022. № 5. С. 226.

4. Бахтеев Д. В. Искусственный интеллект в следственной деятельности: задачи и проблемы // Правовые науки. 2020. № 9. С. 3–6.

Ирада Аллахвердиевна Ганиева,
преподаватель кафедры профессиональной подготовки
Уфимского юридического института МВД России

СЛЕДОВАТЕЛЬ – ЭТО ПРИЗВАНИЕ

Следственная деятельность представляет собой одну из ключевых функций правоохранительной системы любого государства. Следователь должен обладать не только высоким уровнем профессионализма, но и определенными личностными качествами, позволяющими эффективно решать поставленные перед ним задачи. Настоящая статья посвящена рассмотрению особенностей профессиональной деятельности следователя, выявлению специфики этой профессии и определению ее как призвания.

Профессия следователя всегда была окружена ореолом таинственности. Этому в значительной мере способствовало появление детективной литературы, а позже – детективного жанра в кино. Интерес к произведениям о расследованиях необычайно высок во всем мире до сих пор. Стоит только назвать имена Шерлока Холмса, Эркюля Пуаро, мисс Марпл, комиссара Мэгре, Порфирия Петровича, Глеба Жеглова – и сознание выдает знакомые образы, фразы, принадлежащие этим героям, блестяще раскрытые ими дела.

Зачастую герои были лишь плодом художественного вымысла авторов, некими собирательными образами. Позднее, в романах, основанных на реальных событиях, образы следователей стали иметь реальные прототипы, которыми часто являлись сами авторы произведений – бывшие сотрудники органов внутренних дел, много лет посвятившие расследованию преступлений. Личный опыт позволил им наполнить романы реальными фактами и подробностями (такой героиней, например, стала Настя Каменская). Читатели представляют себя на месте прославленных и удачливых сыщиков, выпускники школ идут учиться «на следователя», однако практически никто не представляет, какие требования предъявляет эта профессия к человеку и какими качествами должен обладать следователь-профессионал [1, с. 11].

Следователь играет важную роль в обеспечении правопорядка и правосудия. Его основные обязанности включают расследование преступлений, сбор доказательств, проведение допросов потерпевших, свидетелей и подозреваемых, а также подготовку материалов дела для передачи в суд. Эффективное выполнение этих функций возможно только при наличии глубоких знаний уголовного права, уголовного процесса, криминалистики, психологии и других смежных дисциплин.

Следователь – должностное лицо, уполномоченное в пределах своей компетенции осуществлять предварительное следствие по уголовному делу [2, с. 176]. Это ключевая фигура в системе правоохранительной деятельности.

Следователи играют самую важную роль в расследовании преступлений и защите прав граждан, обращающихся в территориальные органы за помощью. Их деятельность требует высокого уровня профессионализма, ответственности и знания правовых норм. Кроме того, необходимость посещения мест преступлений, следственные действия, давление со стороны руководства, взаимодействие с людьми, имеющими сложный характер, – участниками уголовного судопроизводства – могут влиять на эмоциональное состояние сотрудника следственных органов, и эта дополнительная нагрузка весьма существенна.

К следователю предъявляются высокие требования. Он должен обладать такими важнейшими личностными и профессиональными качествами, как ответственность, справедливость, честность, объективность, исключительная внимательность, умениями анализировать большие объемы информации, делать выводы на основе фактов и принимать решения в условиях неопределенности. Важным качеством является стрессоустойчивость, поскольку работа следователя предполагает необходимость постоянного реагирования на такие проявления эмоций и реалии, как страдание, слезы, боль, насилие, преступления и человеческие трагедии.

Не каждый человек, обладающий названными качествами, способен стать настоящим следователем. Необходимо ощущать неиссякаемый интерес к своему делу, иметь горящие глаза, осознавать, что работа практически не оставит свободного времени, окажется на первом плане, а семья, друзья и родственники – на втором.

В последние годы и даже десятилетия в следственных органах работают женщины, которым свойственна (в отличие от мужчин) усидчивость. К преимуществам женского подхода к работе следователя отнесем и такие уникальные качества, как наличие эмпатии, внимание к деталям и способность выстраивать доверительные отношения с потерпевшими и свидетелями.

Подготовка будущих следователей начинается с обучения в специализированных учебных заведениях, где студенты знакомятся с основами юриспруденции, осваивают криминологию, криминалистику, психологию и другие дисциплины, необходимые для успешной работы в данной сфере. Получив образование, будущие специалисты проходят стажировку под руководством опытных коллег и наставников, что позволяет им приобрести практические навыки и адаптироваться к реалиям следственной работы.

Многие люди выбирают профессию следователя не только из-за интереса к праву и криминалистике. Часто основной причиной является наличие внутреннего чувства долга перед обществом и государством, видение своего жизненного предназначения в защите прав граждан, восстановлении справедливости и борьбе с преступностью. Такая мотивация делает работу следователя не просто профессией, а смыслом жизни для того, кто действительно принял для себя решение служить на благо человечества и Российской Федерации.

Следователь обязан соблюдать права всех участников процесса, в равной мере обеспечивая защиту прав и законных интересов лиц, потерпевших от преступления, и защиту личности от незаконного и необоснованного обвинения, ограничения ее прав и свобод [3, с. 44].

Для успешного выполнения обязанностей следователю необходимо обладать определенными профессиональными и личностными качествами, соответствовать строгим требованиям:

– высшее юридическое образование является обязательным условием для назначения на должность следователя. Специализация должна включать изучение уголовного права, криминалистики, процессуального законодательства и других смежных дисциплин;

– знание правовых норм, глубокое понимание действующего законодательства, особенно Уголовного кодекса Российской Федерации и Уголовно-процессуального кодекса Российской Федерации;

– аналитическое мышление, а именно способность анализировать большие объемы информации, выявлять ключевые факты и делать обоснованные выводы;

– коммуникативные навыки, а именно умение эффективно взаимодействовать с людьми, относящимися к различным категориям, вести переговоры, допросы и опросы;

– стрессоустойчивость (работа следователя связана с необходимостью принимать ответственные решения и действовать в условиях неопределенности);

– честность перед законом и обществом, ответственность за принимаемые решения, соблюдение профессиональной этики.

Деятельность следователя регулируется не только правовыми нормами, но и морально-этическими принципами, важнейшими из которых являются:

– независимость и беспристрастность (следователь должен быть свободным от внешнего давления и принимать решения исключительно на основе закона и имеющихся доказательств);

– соблюдение прав человека (уважение прав всех участников процесса, включая подозреваемых, потерпевших и свидетелей; недопустимо применение пыток, насилия или иных незаконных методов воздействия);

– конфиденциальность (сохранение тайны следствия, недопущение разглашения информации, которая может повлиять на ход расследования или нанести ущерб участникам процесса);

– профессиональная солидарность (сотрудничество с коллегами, обмен опытом и поддержание корпоративной культуры внутри профессионального сообщества).

Профессия следователя требует наличия высокой квалификации, профессиональных знаний, определенных личностных качеств и внутренней мотивации. Это не просто работа, а призвание, требующее полной самоотдачи и постоянного совершенствования. Следователи играют ключевую роль в поддержании правопорядка и обеспечении безопасности жизни общества. Их труд заслуживает глубокого уважения и признания. Эффективная деятельность следователей способствует обеспечению справедливости в обществе и укреплению доверия граждан к правоохранительным органам.

Таким образом, работа следователя – сложный и ответственный вид деятельности – требует постоянного совершенствования профессиональных навыков и соблюдения высоких этических стандартов.

Список библиографических ссылок

1. Основы психологической компетентности в профессиональной деятельности следователя: учеб. пособие для вузов / О. А. Холина, Е. В. Казанцева, В. И. Мищенко. М.: Издательство Юрайт, 2021. 204 с.

2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (в посл. ред.). Доступ из справ.-правовой системы «КонсультантПлюс».

3. Уголовно-процессуальное право Российской Федерации: учеб. / Д. П. Великий, Т. Ю. Вилкова, Л. А. Воскобитова [и др.]. М.: Норма: ИНФРА-М, 2018. 1007 с.

Ольга Александровна Решняк,
доцент кафедры криминалистики
Волгоградской академии МВД России,
кандидат юридических наук, доцент

ОСОБЕННОСТИ ПРИНЯТИЯ САМОСТОЯТЕЛЬНЫХ РЕШЕНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ

Согласно официальным статистическим данным МВД России, преступления против собственности совершаются чаще остальных. Больше половины всех зарегистрированных преступлений (50,5 %) в 2024 г. составили хищения чужого имущества, совершенные путем

– кражи – 499,6 тыс. (–14,3 %),
– мошенничества – 445,7 тыс. (+2,8 %),
– грабежа – 17,6 тыс. (–20,7 %),
– разбоя – 2,8 тыс. (–16,3 %).

Почти каждая девятая кража (10,7 %), каждый двадцать седьмой грабеж (3,8 %) и каждое седьмое разбойное нападение (13,8 %) были сопряжены с незаконным проникновением в жилище, помещение или иное хранилище. В январе – декабре 2024 г. зарегистрировано 14,6 тыс. квартирных краж – на 28,7 % меньше по сравнению с аналогичным периодом прошлого года [1] – в связи с тем, что особое внимание государства и правоохранительных органов уделяется совершенствованию мер борьбы и противодействия преступности данной категории.

Вся деятельность следователя при расследовании преступлений против собственности направлена на установление обстоятельств произошедшего события и выявление следов преступного деяния. Мероприятия, проводимые с этой целью, должны быть четко и грамотно спланированы для получения наиболее эффективного результата. Основную работу при расследовании преступлений против собственности выполняет следователь, руководящий деятельностью следственно-оперативной группы на месте происшествия по горячим следам. Кроме того, после возбуждения уголовного дела следователь принимает его к своему производству и отвечает за результат расследования, действуя исключительно самостоятельно. Такую самостоятельность и процессуальную независимость следователь получил на законодательном уровне: его полномочия регламентированы Уголовно-процессуальным кодексом Российской Федерации (далее – УПК РФ). На основании ст. 38 УПК РФ следователь, являясь процессуально независимым лицом, полномочен самостоятельно определять ход расследования, версии, подлежащие проверке, объем следственных и процессуальных действий, достаточный для составления обвинительного заключения и направления уголовного дела в суд [2].

Работая на месте происшествия по преступлению против собственности в составе следственно-оперативной группы, следователь первым осматривает территорию, оценивает ее состояние, определяет наличие возможных следов и дает указание специалисту-криминалисту об их обнаружении и изъятии. Также он принимает решение о применении наиболее эффективных тактических приемов, оценивает риски и выбирает тактические комбинации, направленные на получение положительного результата.

В настоящее время расследование преступлений против собственности имеет много сложностей: в связи с развитием современных технологий способы и схемы совершения таких преступлений изменились и требуют наличия специальных знаний у следователя. Основной особенностью расследования указанных преступлений является необходимость в незамедлительном принятии следователем самостоятельных решений. Например, получив сообщение о совершении преступления, связанного с хищением денежных средств с банковского счета человека, следователь сразу должен сделать запрос в банк для получения информации о движении денежных средств по счету жертвы. Проанализировав полученные данные, – оперативно запросить информацию о движении денежных средств по счету, на который были переведены денежные средства жертвы, а также принять меры для блокировки данного счета. При установлении лица, совершившего преступление, следователь самостоятельно принимает решение об избрании ему меры пресечения: отпускает его под подписку о невыезде либо ходатайствует перед судом о заключении его под стражу или под домашний арест. Принимая решение об избрании меры пресечения, следователь учитывает тяжесть совершенного преступления, возмещение материального ущерба потерпевшему, личность преступника, его судимости ранее, наличие работы, семьи, постоянного места жительства, состояние здоровья и т. п.

Способность следователя принимать самостоятельные решения основывается на его уверенности в себе, знании законодательства, образованности, твердости в собственных убеждениях, независимости суждений. Решения, принимаемые следователем, должны быть обоснованными, целесообразными, законными, своевременными, оптимальными.

Таким образом, принятие следователем самостоятельных решений при расследовании преступлений против собственности требует проявления положительных качеств личности, следования определенным профессиональным принципам, наличия специальных навыков и высокой степени ответственности.

Список библиографических ссылок

1. Состояние преступности в России за январь – декабрь 2024 года // МВД России: офиц. сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 27.05.2025).

2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (в посл. ред.). Доступ из справ.-правовой системы «КонсультантПлюс».

Татьяна Викторовна Седых,
старший преподаватель кафедры уголовного процесса
и криминалистики Ставропольского филиала
Краснодарского университета МВД России,
кандидат политических наук

ЗНАЧЕНИЕ ЦИФРОВЫХ СРЕДСТВ ФИКСАЦИИ В УГОЛОВНОМ ПРОЦЕССЕ

Цифровые технологии в настоящее время активно применяются в различных сферах, и уголовный процесс исключением не является. Правовое закрепление применения цифровых средств фиксации в уголовно-процессуальном законодательстве регламентируется крайне поверхностно, нет отдельной нормы, посвященной общим условиям применения таких средств. Необходимость ее введения, по нашему мнению, очевидна.

Значение использования видеозаписи и фотосъемки в ходе производства следственных действий с применением цифровых средств фиксации достаточно велико: эти средства позволяют произвести фиксацию определенного объекта, обеспечить сохранность полученных изображений, изготовить необходимое количество копий таких изображений и передать их в любое место.

Цифровая техника имеет высокую стоимость, вследствие чего правоохранительные органы не всегда обеспечиваются средствами, позволяющими качественно запечатлеть объект.

Постепенно в деятельность, связанную с раскрытием и расследованием преступлений, также начинает внедряться цифровизация. Данный процесс происходит медленно, поскольку любые новшества в уголовном судопроизводстве должны быть тщательно исследованы, а их применение – обосновано не только с научной и технической точек зрения, но и с позиции правомерности их использования при доказывании. Всегда остается острым вопрос об обеспечении относимости, допустимости, достоверности полученных сведений, поэтому применение любых технических средств, каковыми являются и цифровые средства фиксации, должно иметь соответствующую правовую основу. При наличии ее и выполнении соответствующих функций специалисты могут решать определенные задачи:

– обеспечение возможности следователя, дознавателя не отвлекаться от производства следственного действия, наблюдая за реакцией его участников, верно отражая в протоколе ход и результаты следственного действия;

– осуществление более качественной фиксации следственного действия (специалист в большей степени обладает тактическими приемами применения фото и видеозаписи, и это позволит исключить ошибки при фиксации изображений объектов).

К примеру, следователи, нередко производящие фотографирование похищенного, а затем обнаруженного и изъятого предмета самостоятельно, снимают лишь его общий план, и серийный номер на изображении разглядеть оказывается невозможно. В случае производства следственного эксперимента и проверки показаний на месте, когда фотографирование или видеосъемку производит следователь, нередко упускаются ключевые моменты, обстановка фиксируется не в полном виде.

Определенные требования к применению цифровых средств технической фиксации выработаны в ходе правоприменительной практики, поскольку закон не со-

держит необходимых разъяснений. Так, например, руководствуясь тем, что любые доказательства должны отвечать требованиям достоверности и допустимости, следствие не может использовать цифровые средства фиксации, не прошедшие сертификацию, поскольку нет гарантии того, что информация будет фиксироваться ими без искажений [1]. Указанное требование должно найти свое законодательное закрепление.

Средства цифровой фиксации при использовании их в уголовном судопроизводстве играют важную роль, так как позволяют наглядно отразить ход и результаты расследования, сохранить полученную информацию без искажения и при необходимости многократно ее использовать. Те возможности, которые предоставляет следователю, дознавателю, суду и иным участникам уголовного судопроизводства применение цифровых средств фиксации информации, должны использоваться в полной мере, но только при условии, что это отвечает требованиям уголовно-процессуального законодательства. В настоящее время такие требования минимальны, четко определено лишь, что в случае применения рассматриваемых средств следователь, дознаватель должны уведомить об этом участников следственных действий и отразить факт применения технических средств фиксации (в том числе цифровых) в протоколе. Полагаем, что такой подход не позволяет в полной мере обеспечить допустимость доказательств информации, получаемой при применении цифровых средств фиксации лицами, производящими расследование. Необходимо четкое законодательное регулирование требований, предъявляемых к цифровым средствам фиксации, и порядка их применения.

Анализ научных источников и судебной практики позволяет сделать вывод о том, что при проведении экспертиз и исследований средства цифровой видеофиксации практически не применяются, преимущественно используется цифровая фотография, причем на всех стадиях исследования [2].

Первая стадия – подготовительная – предназначена для того, чтобы эксперт мог ознакомиться с поступившим постановлением о назначении судебной экспертизы, а также объектами, которые предоставлены эксперту. На данной стадии эксперт изучает постановление, проверяя, соответствует ли оно всем требованиям, содержится ли в нем необходимая ему информация, выясняя, какие вопросы перед ним поставлены и может ли он на них ответить [3]. После изучения постановления о назначении экспертизы происходит ознакомление с объектами, поступившими на экспертизу. Эксперт проверяет их достаточность, а также в обязательном порядке – упаковку данных объектов. На них должно быть указано, какие именно объекты представлены, как и где они были получены. На упаковке объектов, помимо пояснительных надписей, должны находиться подписи. С помощью цифровых средств и фотографирования осуществляется фиксация представленных объектов – таким образом, чтобы все, указанное на упаковке, было запечатлено.

В обязательном порядке должна быть проверена целостность упаковки объектов, поступивших на экспертизу. Специалисту необходимо удостовериться в том, что упаковка, выполненная надлежащим образом, не была нарушена. Данный факт также фиксируется. Такой подход позволяет избежать ошибок и неточностей, поскольку описание в заключении эксперта предоставленных объектов и их внешнего вида (упаковки) должно совпадать с изображениями на фото, прилагающихся в качестве фототаблицы к заключению эксперта. Осмотру и фотофиксации подлежат и сами объекты: они должны в полной мере совпадать с теми, которые указаны в постановлении о назначении экспертизы. Это позволяет минимизировать возможность случайно перепутать объекты, прилагаемые к постановлениям (подобное

может произойти, к примеру, когда следователь назначает несколько судебных экспертиз по разным уголовным делам).

Средства цифровой фотофиксации в обязательном порядке применяются непосредственно в ходе судебной экспертизы, то есть на стадиях, следующих за подготовительной.

В уголовном судопроизводстве давно и активно используются различные технические средства фиксации.

Наиболее часто при производстве следственных действий применяется цифровое фотографирование. При этом используются выработанные наукой и апробированные способы и методы фотографирования и видеозаписи, что позволяет обеспечить оптимальное качество получаемого изображения.

Использование фото- и видеофиксации позволяет лицам, не принимающим участие в следственном действии, представить ход его производства и ознакомиться с полученными результатами. Можно говорить о недостаточности существующей правовой основы использования технических средств в уголовном судопроизводстве. Те фрагменты положений Уголовно-процессуального кодекса Российской Федерации, в которых содержится указание на особенности использования технических средств в уголовном процессе, не могут обеспечить достижение четкого понимания правоприменителями, каким образом надлежит использовать в ходе расследования технические средства, включая цифровые средства фиксации. Необходимо четкое законодательное регулирование как требований, предъявляемых к цифровым средствам фиксации и порядку их применения, так и процедуры приобщения полученных результатов к материалам уголовного дела, а также оценки доказательств, полученных рассматриваемым способом.

Список библиографических ссылок

1. Васильева М. А., Лебедева А. А. Криминалистические аспекты использования цифровых способов фиксации следов при расследовании преступлений // Вопросы российского и международного права. 2019. Т. 9. № 9-1. С. 219–225.

2. Ростовцев А. В. Правовые, организационные и методические вопросы применения цифровых технологий при производстве судебных экспертиз // Вестник Московского университета МВД России. 2014. № 10. С. 124–126.

3. Эджубов Л. Г., Микляева О. В. Стадии экспертного исследования // Энциклопедический словарь теории судебной экспертизы: сб. ст. / под ред. С. А. Смирновой. М.: Федеральное бюджетное учреждение «Российский федеральный центр судебной экспертизы имени профессора А. Р. Шляхова при Министерстве юстиции Российской Федерации», 2012. Ч II. С. 336–338.

Алиса Джамаловна Смыр,
адъюнкт адъюнктуры
Волгоградской академии МВД России

ОСОБЕННОСТИ РЕГЛАМЕНТАЦИИ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ ПО ЗАКОНОДАТЕЛЬСТВУ ДОРЕВОЛЮЦИОННОЙ РОССИИ

Становление и развитие ответственности за преступления в сфере транспорта осуществлялись долго и сложно – в непосредственной связи с эволюцией транспортных средств, инфраструктуры и правовой мысли. Анализ законодательных актов в дореволюционной России позволяет проследить, как государство реагировало на возникающие угрозы безопасности движения и определяло нормы эксплуатации транспортных средств, постепенно формируя систему правовых запретов и санкций.

Первое упоминание об ответственности за действия, связанные с транспортом, можно обнаружить в древнерусском праве. Русская Правда уделяла внимание охране лошадей как важнейшего элемента хозяйства, устанавливая суровые наказания за их кражу и незаконное пользование. В то время гужевые повозки были единственным видом транспорта. Однако нормы, непосредственно регулирующие безопасность передвижения гужевого транспорта, отсутствовали.

В Судебнике 1497 г. (ст. 30 «Указ о езду») была предпринята попытка регулирования безопасности на транспорте. В указанной норме закреплялось поощрение в денежном эквиваленте за пройденное «неделщиком» от Москвы до других городов Руси расстояние [1, с. 80].

Соборное уложение 1649 г. (далее – Уложение) сделало значительный шаг в развитии законодательства в сфере транспорта того времени. В ст. 17 гл. XXII значилось: «А будет кто с похвалы или с пьянства, или умыслом наскачет на лошади на чью жену, и лошадью ея стопчет и повалит, и тем ея обесчестит, или ея тем боем изувечит, и беременная будет жена от того его бою дитя родит мертво, а сама будет жива, а с суда сыщется про то допряма, и тому, кто так учинит, за такое его дело учинити жестокое наказание, велеть его бити кнутом нещадно, да на нем же доправити той жене бесчестие и увечье вдвое, да его же вкинути в тюрму на три месяца. А будет от того его бою та жена и сама умрет, и его за такое его дело казнити смертию» [2, с. 249]. Нельзя не отметить, что Уложение разграничивало умышленные и неосторожные деяния, а также предусматривало квалифицирующие признаки, влияющие на вид наказания. Не считалось виной причинение смерти потерпевшему от действий наездника, который не смог остановить лошадь, но сделал все возможное для этого, «потому что лошадь от чего испужався, и узду изорвав разнесет, и удержати ея будет немощно» [3]. Стоит также отметить, что в Уложении 1649 г. есть гл. IX «О мытах и о перевозех, и о мостах», регулирующая систему перевозок, содержание мостов, а также порядок содержания дорог [2, с. 100].

С ростом городов и увеличением численности населения и интенсивности движения возникла необходимость в установлении специальных правил, обеспечивающих безопасность на транспорте, а также ответственность за пренебрежение этими правилами и нарушение их. Такие положения были закреплены в указах Анны Иоанновны (1730 г.) и Елизаветы Петровны (1742 г.). Эти акты обязывали не только извозчиков, но и других лиц передвигаться на лошадях с особой осторожностью, а для тех, кто не соблюдал эти правила, были установлены наказания разной степени

тяжести – от битья кнутом до каторги. Спустя некоторое время в последний документ были внесены дополнения. К таковым, например, относится следующее: «Если кто на резвых лошадях ездить будет, тех через полицейские команды ловить и лошадей их отсылать в конюшню государыни» [2, с. 137].

Подписанный в 1775 г. Манифест Екатерины II определял виды экипажей и количество лошадей, должное находиться в упряжке. Наложение строгих мер для обеспечения безопасности на дорогах не искореняло нарушение правил движения, приводившее к гибели и травмам людей. Аварии в то время происходили также вследствие неправильной эксплуатации экипажей. В связи с этим Устав г. Санкт-Петербурга 1798 г. впервые закрепил обязанность полиции контролировать техническое состояние транспортных средств. Это стало важным шагом в направлении технической регламентации [3].

Эти ранние нормативные акты заложили основу для дальнейшего развития уголовно-правовых мер обеспечения транспортной безопасности.

Вопросам безопасности движения в XIX в. стало уделяться еще больше внимания. Сельский Судебный Устав для государственных крестьян 1839 г. «за скорую езду по улицам, базарам, ярмаркам и другим местам, часто людьми посещаемым, в случае происшедшего от сего вреда другому» [4, с. 305] предусматривал уголовную ответственность, совершение данного вида преступления наказывалось штрафом или заключением под стражу.

Появление в Российской империи новых транспортных средств стало причиной принятия новых правовых норм, связанных с запретами нарушений правил дорожного движения и эксплуатации транспортных средств. Уложение о наказаниях уголовных и исправительных 1845 г. содержало в себе большее в сравнении с упомянутыми ранее нормативно-правовыми актами количество статей, непосредственно связанных с транспортом. Этот уголовный кодекс предусматривал ответственность за дорожно-транспортные происшествия, становившиеся причиной несчастных случаев или повреждений дорожного покрытия. Термином «приключение» [5, с. 14] называются здесь вредные последствия.

Принятие в 1864 г. Устава «О наказаниях, налагаемых мировыми судьями» стало еще одним важным шагом на пути становления ответственности за совершение транспортных преступлений. В данном нормативном акте содержалась ст. 73, согласно которой за «препятствование проходу по мосткам и тротуарам или проезду по дорогам и улицам оставлением на них громоздких предметов или иным образом» [2] предусматривалась ответственность в виде штрафа.

Уголовное уложение 1903 г. наряду с основными составами преступлений, определяющими ответственность за транспортные преступления, включало в себя квалифицированные составы. К ним в тот период относились создание опасности для жизни и здоровья людей, разрушение рельсового транспорта, парохода, судна. Следует подчеркнуть, что уже в то время рассматриваемый вид преступления считался формальным. Уложение 1903 г. дифференцировало ответственность в зависимости от вида транспорта (железнодорожный, водный, наземный) и субъекта преступления (служащие, начальствующий состав, пассажиры, иные лица). Были криминализированы различные виды нарушений правил эксплуатации транспортных средств и содержания путей сообщения. В случае причинения смерти или вреда здоровью вследствие нарушения правил безопасности предусматривалась ответственность за неосторожные преступления, а также впервые вводилась возможность лишения права заниматься определенной деятельностью [6, с. 507].

Уложение 1903 г., хотя и не вступило в полном объеме в законную силу, все-таки оказало значительное влияние на содержание связанных с транспортными преступлениями нормативно-правовых актов постреволюционного периода.

Таким образом, в дореволюционной России поэтапно создавалось законодательство, устанавливающее ответственность за нарушение транспортной безопасности. При известных неполноте и казуистичности рассмотренных выше норм они являлись основой для зарождения в российском уголовном праве института транспортных преступлений. Преимущественно формальный характер составов преступлений подчеркивал высокую общественную значимость охраны отношений в исследуемой сфере, не утратившую своей актуальности и сегодня.

Список библиографических ссылок

1. Российское законодательство X–XX веков: в 9-ти томах / под общ. ред. О. И. Чистякова. Т. 2: Законодательство периода образования и укрепления Русского централизованного государства / отв. ред. А. Д. Горский. М.: Юридическая литература, 1985. 519 с.

2. Российское законодательство X–XX веков: в 9-ти томах / под общ. ред. О. И. Чистякова. Т. 3: Акты земских соборов конца XVI – начала XVII века. Соборное уложение 1649 года. Акты Земских соборов 50-х годов / отв. ред. А. Г. Маньков. М.: Юридическая литература, 1985. 511 с.

3. Горбунова Л. В. Некоторые аспекты развития законодательства об ответственности за преступления против безопасности движения и эксплуатации транспорта в дореволюционной России // Марийский юридический вестник. 2008. Вып. 6. С. 105–108.

4. Полное собрание законов Российской империи. Собрание 2-е. Т. XIV. Отделение первое. 1839. Спб.: Типография II Отделения Собственной Е. И. В. Канцелярии, 1840. 1185 с.

5. Любимов Л. В. Дорожно-транспортные преступления: проблемы законодательного конструирования составов и дифференциации ответственности участников дорожного движения: дисс. ... канд. юрид. наук: 12.00.08 / Любимов Леонид Вячеславович. Волгоград, 2005. 234 с.

6. Полный курс уголовного права. Т. 4: Преступления против общественной безопасности / В. С. Комиссаров, А. И. Коробеев. СПб.: Юридический центр Пресс, 2008. 672 с.

Олег Валентинович Стрилец,
профессор кафедры уголовного права
учебно-научного комплекса
по предварительному следствию
в органах внутренних дел
Волгоградской академии МВД России,
кандидат юридических наук, доцент,

Виктория Геннадьевна Олесовец,
адъюнкт адъюнктуры
Волгоградской академии МВД России

ПРОБЛЕМЫ НАЗНАЧЕНИЯ НАКАЗАНИЙ В УГОЛОВНО-ПРАВОВОЙ ДОКТРИНЕ

В уголовно-правовой доктрине проблемы назначения наказания традиционно относятся к числу фундаментальных. Будучи ключевым элементом уголовной ответственности, наказание представляет собой сложный социально-правовой институт, эффективность которого зависит от множества факторов. Теоретические вопросы назначения наказания касаются как общих принципов его назначения, так и специфических задач, связанных с индивидуализацией ответственности: учета обстоятельств, смягчающих или отягчающих наказание; применения альтернативных видов наказаний; отсутствия нижнего порога наказания в санкциях отдельных статей Особенной части Уголовного кодекса Российской Федерации и т. д.

Большинство исследователей и ученых солидарны в том, что наказание, являясь мерой государственного принуждения, устанавливается от имени государства по приговору судов виновным лицам для достижения целей общей и специальной превенции [1, с. 29].

Вместе с тем серьезной проблемой является противоречивость целей, преследуемых наказанием. С одной стороны, наказание должно быть возмездием за причиненный вред, восстанавливающим нарушенную справедливость. С другой стороны, оно должно способствовать исправлению осужденного, его ресоциализации и возвращению к законопослушной жизни. Наконец, наказание должно выполнять превентивную функцию, удерживая от совершения преступлений как самого осужденного, так и других лиц.

Назначение несправедливого наказания за тяжкое преступление может препятствовать исправлению осужденного и его успешной реинтеграции в общество после освобождения. И наоборот, гуманистический подход, ориентированный на ресоциализацию, может быть воспринят как проявление слабости и неспособности государства защитить своих граждан от преступных посягательств. Разрешение этого противоречия требует от суда взвешенного подхода, учета всех обстоятельств дела и умения находить компромисс между различными целями наказания [2].

Одним из вопросов, обсуждаемых в доктрине уголовного права в части, касающейся назначения наказания, является учет обстоятельств, смягчающих и отягчающих наказание в аспекте прав и обязанностей суда.

Существуют сторонники оставления за судом права самостоятельного учета смягчающих и отягчающих обстоятельств. Например, А. А. Мясников отмечает: «Будучи лишь частью родового института назначения наказания, правила смягче-

ния наказания дополняются предписаниями относительно его возможного ужесточения. Эти два института как бы «уравновешивают» друг друга, выступая необходимым дополнением общих начал назначения наказания» [3, с. 183]. При этом стоит согласиться с мнением Л. Л. Кругликова, который считает, что принять во внимание комплекс обстоятельств не означает обязательно снизить наказание [4, с. 5].

Противоположной точки зрения придерживаются А. Рарог и Е. Акимова, полагающие, что неосновательное расширение функций судебных органов за счет сужения функций законодателя неосновательно, влечет ухудшение правового положения правонарушителя» [5, с. 27].

Представляется целесообразным закрепить на законодательном уровне отягчающие и смягчающие обстоятельства.

В последние годы все больше внимания уделяется альтернативным видам наказаний, не связанным с лишением свободы. Однако их применение на практике встречает ряд проблем. Некоторые виды альтернативных наказаний применяются судами крайне редко. Например, лишение права занимать определенные должности или заниматься определенной деятельностью в 2024 г. назначено судами Российской Федерации всего в 89 случаях, при этом обязательные работы – в 64 723; штраф – в 78 585 [6].

Ряд ученых ссылается на недостаточную правовую регламентацию некоторых видов альтернативных наказаний (например, ограничение свободы имеет недостатки нормативных предписаний, затрудняющих его исполнение [7, с. 80]), другие – на трудности исчисления срока альтернативного наказания по совокупности преступлений (в частности, когда за одно из преступлений назначен штраф, а за другое – обязательные работы) [8, с. 26].

Говоря об исправительных работах, отметим, что круг назначения данного вида наказаний максимально расширился в 2011 г., когда стало возможным назначать этот вид наказания вне зависимости от наличия основного места работы (ст. 27 Уголовного кодекса РСФСР 1960 г. содержала аналогичные положения, что свидетельствует об исторической преемственности [9, с. 176]).

Применение наказания, не связанного с изоляцией от общества, с привлечением осужденного к труду, несомненно, способствует снижению уровня рецидивной преступности, поэтому такие виды наказания (например, исправительные работы) применяются судами достаточно часто.

Однако на практике существуют проблемы применения данного вида наказания к тем лицам, которые не имеют официального места работы.

Осужденный должен выполнять исправительные работы в районе места жительства, вместе с тем в реальности возможность трудоустроиться есть не во всех населенных пунктах, а самостоятельное трудоустройство вне территории проживания осужденного будет нарушением законодательства и, как следствие, повлечет увольнение такого работника. С одной стороны, осужденному предоставлена возможность отбывания наказания более мягкого и гуманного в сравнении с некоторыми иными видами наказания, с другой стороны, эта возможность трудно реализуема практически, поскольку порядок определения мест отбывания исправительных работ не эффективен.

Наказание должно отбываться только в тех местах, которые определяют органы местного самоуправления по согласованию с уголовно-исполнительными инспекциями, однако часто эти учреждения вынуждены отказывать в трудоустройстве ввиду недостатка рабочих мест. Для повышения эффективности реализации данного вида наказания правоведы, такие как Б. А. Спасенников, И. В. Дворянсков, А. В. Но-

виков и др., предлагают привлекать службы занятости населения [10]. Это предложение заслуживает внимания, поскольку именно центры занятости населения обладают необходимым инструментарием для трудоустройства, в частности, аккумулируют информацию о вакантных рабочих местах.

Действующее законодательство содержит ограничения назначения исправительных работ отдельным категориям осужденных (инвалиды первой группы, женщины (беременные и имеющие детей в возрасте до трех лет), военнослужащие по призыву). Кроме того, такой вид наказания не назначается при осуждении за определенные категории преступлений, в частности, за тяжкие и особо тяжкие составы (убийство, умышленное причинение тяжкого вреда здоровью, сбыт наркотических средств и др.).

Множество проблем и споров вызывает отсутствие в Уголовном кодексе Российской Федерации нижнего предела наказания за совершение преступления. Такой подход по своей сути означает, что суд, признавший подсудимого виновным в совершении преступления, при вынесении решения не ограничен минимальным сроком или размером наказания, установленным в санкции статьи. Судья имеет дискреционное право определять наиболее адекватную и справедливую меру государственного принуждения, исходя из индивидуальных обстоятельств дела, личности преступника и степени общественной опасности содеянного. Данная законодательная позиция несет в себе потенциальные риски. Во-первых, существует опасность субъективного подхода к определению наказания. Разные судьи могут по-разному оценивать одни и те же обстоятельства дела, что приведет к принятию несоразмерных и непредсказуемых решений. Во-вторых, возникает риск коррупции и злоупотреблений. Судьи, обладающие широким дискреционным правом, могут быть подвержены давлению со стороны заинтересованных лиц. В-третьих, отсутствие четких ориентиров в определении наказания способно снизить сдерживающий эффект уголовного закона. Преступники, не знающие, какое наказание их ждет в случае совершения преступления, могут быть менее склонны воздерживаться от противоправных действий.

Так, санкция ч. 4 ст. 111 Уголовного кодекса Российской Федерации, устанавливающая наказание за причинение тяжкого вреда здоровью, повлекшего по неосторожности смерть потерпевшего, не содержит нижнего предела наказания. Ранее за указанное преступление нижний порог наказания был установлен – 5 лет лишения свободы.

Такие нововведения имеют определенные негативные последствия: они подрывают общественное доверие к существующей системе правосудия, снижают значимость принципов законности и справедливости, препятствуют формированию единообразной судебной практики.

Отсутствие нижнего предела наказания приводит к неопределенности и применению норм на судейское усмотрение, то есть инициирует использование предоставленных судье уголовно-правовыми нормами правомочий по выбору решения в пределах, установленных законом, в соответствии с его правосознанием и волей законодателя, исходя из принципов права и конкретных обстоятельств совершения преступления [11, с. 37].

Дискуссия о проблемах назначения наказания является одной из наиболее сложных и актуальных в уголовном праве. От обоснованного назначения наказания зависит обеспечение справедливости, восстановление нарушенных прав и интересов потерпевшего, предупреждение совершения новых преступлений. Решение этих проблем требует комплексного подхода, включающего совершенствование законода-

тельства, развитие альтернативных видов наказаний, повышение эффективности деятельности пенитенциарной системы. Важно помнить, что наказание должно быть не только справедливым, но и эффективным в плане достижения своих целей.

Список библиографических ссылок

1. Сундуров Ф. Р., Талан М. В. Наказание в уголовном праве: учебное пособие. М.: Статут, 2015. 256 с.

2. Стрилец О. В. Эффективность целей наказания в новейшей российской истории // Уголовное законодательство: вчера, сегодня, завтра: материалы ежегодной Междунар. науч.-практ. конф., Санкт-Петербург, 7–8 июня 2024 г. / под ред. Т. А. Огарь, Д. М. Кокина; сост. Ю. А. Шутова. СПб.: Санкт-Петербургский университет МВД России, 2024. С. 227–230.

3. Мясников А. А. Понятие и общая характеристика института смягчения наказания // Общество и право. 2010. № 4 (31). URL: https://cyberleninka.ru/article/n/ponyatie-i-obschaya-harakteristika-instituta smyagcheniya-nakazaniya (дата обращения: 20.03.2025).

4. Кругликов Л. Л. Практика учета судами смягчающих и отягчающих обстоятельств при назначении наказания // Пенитенциарная наука. 2014. № 1 (25). URL: https://cyberleninka.ru/article/n/praktika-ucheta-sudami-smyagchayuschih-i-otyagchayuschih-obstoyatelstv-pri-naznachenii-nakazaniya-1 (дата обращения: 20.03.2025).

5. Рарог А., Акимова Е. Назначение наказания. Верховный Суд разрешил вопросы, накопившиеся после принятия УК, но уже возникли новые // Российская юстиция. 1999. № 11. С. 27.

6. Судебный департамент при Верховном Суде Российской Федерации // Судебная статистика: офиц. сайт. URL: http://www.cdep.ru/ (дата обращения: 12.05.2025).

7. Непомнящая Т. В. Проблемы назначения уголовных наказаний, альтернативных лишению свободы // Правоприменение. 2018. Т. 2. № 2. С. 80–89.

8. Хромых Е. В. Альтернативные лишению свободы уголовные наказания: теория и практика назначения и исполнения: автореф. дисс. ... канд. юрид. наук: 12.00.08 / Хромых Евгений Викторович. Ростов-на-Дону: Рост. юрид. ин-т МВД России, 2005. 26 с.

9. Подройкина И. А. Исторические традиции и преемственность построения системы уголовных наказаний // Наука и образование; хозяйство и экономика; предпринимательство; право и управление. 2012. № 4. С. 176–181.

10. Новиков А. В., Габраев А. Ш. Проблемы организации и правового регулирования исполнения наказания в виде исправительных работ // Современные проблемы науки и образования. 2015. № 2–1. URL: https://science-education.ru/ru/article/view?id=21358 (дата обращения: 20.03.2025).

11. Грачева Ю. В. Судейское усмотрение в реализации уголовно-правовых норм: проблемы законотворчества, теории и практики: автореф. дисс. ... д-ра юрид. наук: 12.00.08 / Грачева Юлия Викторовна. М.: Московская государственная юридическая академия имени О. Е. Кутафина, 2011. 38 с.

Анна Викторовна Сычева,
доцент кафедры криминалистики
Волгоградской академии МВД России,
кандидат юридических наук

СПЕЦИФИКА РАССЛЕДОВАНИЯ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

Человека в современном мире уже невозможно представить без компьютеров, планшетов, телефонов, социальных сетей. Жизнь людей становится комфортной, однако появляется и много угроз. С развитием мобильных сетей, доступности подключения телефонов к сети Интернет и появлением возможности перечисления денежных средств с помощью мобильных устройств и приложений сложились оптимальные условия для дистанционного мошенничества [1]. Проблема роста количества случаев его совершения на территории России по-прежнему является острой. Об этом в своем выступлении заявил министр внутренних дел Российской Федерации В. А. Колокольцев, выступая на расширенном заседании коллегии МВД России 5 марта 2025 г. Известно, что мошенники постоянно придумывают новые способы совершения преступлений, оптимизируют существующие. Рассмотрим некоторые способы, реализуемые ими в современных условиях.

Так, мошенники модифицировали хорошо известный алгоритм распространения вредоносного программного обеспечения. Они находили YouTube-блогеров, разместивших в описании видеороликов ссылки для скачивания программного обеспечения, а затем, представляясь правообладателями и угрожая составлением жалоб на канал, требовали заменить «некорректную» ссылку на «правильную». По «правильной» пользователи скачивали архив с майнером SilentCryptoMiner[1], который в скрытом режиме использовал ресурсы устройства и трафик для добычи криптовалюты. Естественно, денежные средства получал не хозяин компьютера, а мошенники [2].

Давно известный способ совершения мошенничества посредством генерации фиктивных QR-кодов применяли мошенники в течение длительного периода в крупной торговой сети г. Москвы. При оплате на кассах самообслуживания преступники генерировали фиктивные штрих-коды. Это позволяло приобретать товары со значительной скидкой. По выявленным фактам возбуждено 16 уголовных дел по признакам составов преступлений, предусмотренных ст. 159 Уголовного кодекса Российской Федерации (далее – УК РФ) [3].

На территории Башкортостана, Татарстана и Краснодарского края мошенники использовали разработанное ими специализированное программное обеспечение, которое в автоматическом режиме с помощью технологии искусственного интеллекта заполняло электронные опросные листы покупателей. Покупка произвольным покупателем определенного вида товара сразу же «привязывалась» к одной из находившихся под контролем мошенников карт лояльности. После этого держателю карты направлялась анкета с предложением оценить работу торгового объекта. Целью преступников было повышение рейтинга определенных магазинов и необоснованное начисление премий их директорам, являвшимся соучастниками преступлений. Впоследствии денежные средства распределялись между всеми членами организованной группы. В ходе предварительного расследования при проведении обысков

[1] Майнеры – приложения по добыче (майнингу) криптовалюты. Запускаются без ведома хозяина. Добытая криптовалюта поступает в распоряжение преступника.

по месту жительства преступников были обнаружены и изъяты более 4,5 тыс. карт лояльности, компьютерная техника и средства связи [4].

Мошенники постоянно осуществляют хакерские атаки на различные организации. Так, в ходе одной из них военная разведка Украины получила неправомерный доступ к информационным ресурсам Учебно-методического центра военно-патриотического воспитания молодежи «Авангард» и Всероссийского детско-юношеского военно-патриотического общественного движения «Юнармия». Действия сотрудников военной разведки Украины преследовали основную цель – осуществить сбор персональных данных подростков для их дальнейшей вербовки и вовлечения в разведывательно-подрывную деятельность против безопасности России, а также совершения диверсионно-террористических актов на территории России. Хакерская атака была локализована [5].

Активно развивается мошенничество с инвестициями. Так, М. с ноября 2022 г. создал в мессенджере группу по инвестированию цифровой валюты в NFT бизнес-проект[1]. Мошенник выдавал себя за успешного криптоинвестора, обещал потенциальным «партнерам» сверхдоходные инвестиции в NFT-картины своего знакомого художника. Затем он добавлял присоединившихся к «участию» в проекте в чат, где якобы размещалась информация о сделках. После получения права собственности на цифровую валюту М. переставал выходить на связь. Похищенную криптовалюту он переводил на заранее созданные цифровые кошельки [6].

Введенное государством с 1 марта 2025 г. право граждан на оформление самозапретов на получение кредитов мошенники также успешно стали применять в целях получения незаконной выгоды. Мошенники оперативно реагируют на актуальные новости, адаптируя «скрипты»[2] или изобретая новые способы совершения мошенничества. Преступники звонят потенциальным жертвам, представляясь сотрудниками портала «Госуслуги», и уверяют, что запрет был установлен неверно. Далее жертве посредством мессенджера направляют фишинговую ссылку якобы для того, чтобы исправить заявление. Перейдя по указанной ссылке, человек попадает на фишинговый сайт портала «Госуслуги», вводит там свои данные для входа. Данные перехватываются мошенниками, и преступники могут авторизоваться в приложении банка с помощью портала «Госуслуг», а затем получить доступ к счетам жертвы. Кроме того, по фишинговой ссылке на устройство пользователя может быть загружен вирус, способный считывать СМС-сообщения, в том числе одноразовые коды для входа на сайт «Госуслуги» или в приложение банка.

Сведения о способе совершения дистанционного мошенничества могут помочь следователю спланировать расследование преступления, выдвинуть правильную следственную версию и отработать ее, установить личность преступника в целях скорейшего раскрытия преступления.

---

[1] NFT, или невзаимозаменяемый токен, – это единица учета, с помощью которой создается цифровой слепок для уникального предмета – картины, фотографии, видео, музыки, гифки. Такие предметы – большая ценность среди коллекционеров, геймеров и любителей искусства. Покупают и продают их через аукционы. URL: https://journal.sovcombank.ru/glossarii/nft-prostimi-slovami-chto-eto-i-kak-na-nem-zarabotat (дата обращения: 18.03.2025).

[2] Скрипт – небольшая программа, выполняющая конкретную задачу. Обычно у скриптов нет своего визуального интерфейса: это код, который запускается по команде, отрабатывает, совершает нужные действия и завершается. URL: https://blog.skillfactory.ru/glossary/skript/ (дата обращения: 18.03.2025).

Список библиографических ссылок

1. Антонян Ю. М. Социальная психология: учебник для высших учебных заведений. М.: Аспект Пресс, 2021.

2. Мошенники научились майнить криптовалюту через YouTube-блогеров. URL: https://ntr-24.ru/news/technologies/129682-moshenniki-nauchilis-majnit-kriptovaljutu-cherez-youtube-blogerov.html (дата обращения: 18.03.2025).

3. МВД ликвидировало деятельность кибермошенников, подделавших штрих-коды. URL: https://tass.ru/obschestvo/23315345 (дата обращения: 18.03.2025).

4. В Татарстане выявили мошенничество с использованием карт лояльности. URL: https://finance.rambler.ru/money/54298706-v-tatarstane-vyyavili-moshennichestvo-s-ispolzovaniem-kart-loyalnosti/ (дата обращения: 18.03.2025).

5. ФСБ сообщила о взломе ресурсов центра «Авангард» и «Юнармии» для вербовки учащихся. URL: https://www.interfax.ru/russia/1012237 (дата обращения: 18.03.2025).

6. Создателя NFT-проекта Илью Малова приговорили к 6 годам за мошенничество. URL: https://www.kommersant.ru/doc/7564177 (дата обращения: 18.03.2025).

Денис Валентинович Теткин,
доцент кафедры уголовного процесса Рязанского филиала
Московского университета МВД России имени В. Я. Кикотя,
кандидат юридических наук

ПРОБЛЕМАТИКА ИСПОЛЬЗОВАНИЯ СИСТЕМ ВИДЕО-КОНФЕРЕНЦ-СВЯЗИ В ПРОЦЕССЕ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ

Процесс внедрения в уголовное судопроизводство современных достижений научно-технического прогресса напрямую связан с определением их эффективности. Стоит отметить, что использование технологий необходимо не только для противодействия новым видам преступления, но и для совершенствования существующей системы расследования преступлений – для получения доказательств или проведения следственных действий, в частности, на досудебной стадии.

Федеральный закон от 30 декабря 2021 г. «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» стал регулировать вопросы проведения допроса, очной ставки, а также опознания посредством использования систем видео-конференц-связи (далее – ВКС). Подобные изменения вызвали активные споры в научном мире.

Предполагается, что в ходе реализации положений указанного Федерального закона проведение следственных действий с использованием систем ВКС позволит сократить время проведения таковых действий, что, в свою очередь, положительно повлияет на соблюдение сроков расследования уголовного дела, минимизирует продление сроков предварительного следствия.

Одним из основных проблемных моментов является отсутствие законодательного регулирования термина «видео-конференц-связь». Некоторые ученые высказывают мнение, согласно которому нормативно-правовое регулирование указанной дефиниции должно найти свое отражение в ст. 5 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ). Так, С. Д. Долгинов справедливо отмечает, что в целях устранения двусмысленности в возможных толкованиях понятие «видео-конференц-связь» должно найти отражение в п. 4.1. ст. 5 УПК РФ [1, с. 474]. Мы согласны с обозначенной точкой зрения и считаем, что под термином «видео-конференц-связь» необходимо понимать использование технических средств для осуществления законодательно закрепленных процессуальных действий, обеспечивающее дистанционное взаимодействие участников уголовного судопроизводства в режиме реального времени.

Рассуждая о необходимости внедрения видео-конференц-связи на стадии предварительного следствия, обозначим положительные и негативные стороны.

К положительным относится психологический компонент, возникающий при проведении допроса посредством использования видео-конференц-связи. Традиционный способ проведения допроса состоит в непосредственной беседе следователя и допрашиваемого лица, в ходе которой становится известна информация, связанная с предметом доказывания. В таком случае лицо, дающее показания, может почувствовать давление со стороны следователя, неуверенность в собственных словах ввиду влияния фактора времени и иного.

Для решения подобного рода проблем стоит использовать видео-конференц-связь. О. С. Пашутина и Д. В. Алымов высказали точку зрения, согласно которой

использование систем видео-конференц-связи при производстве следственных действий, касающихся несовершеннолетних участников, позволит допрашиваемым в психологически комфортной обстановке дать показания об известных им обстоятельствах [2, с. 15]. Выражая согласие с приведенным мнением, отметим, что нахождение допрашиваемого лица в комфортной для него обстановке в действительности благоприятно влияет на исход проводимого следственного действия.

Помимо сказанного, несомненным преимуществом является удобство проведения следственных действий для их участников: исключается необходимость явки в территориальные органы внутренних дел, что позволяет сократить время на проведение следственного действия, в режиме реального времени фиксируется информация, предоставляемая лицами, не имеющими возможность находиться по месту проведения допроса, очной ставки, опознания.

Одним из следственных действий, в ходе которого может быть применена система ВКС, является очная ставка. Ее суть состоит в проведении одновременного допроса двух лиц, при этом вопросы могут задавать и следователь, и участники проводимого следственного действия. Задача заключается в устранении противоречий в показаниях лиц. Отмечается, что важность очной ставки обусловлена возможностью оказания психологического воздействия участников друг на друга. Член Совета Федеральной палаты адвокатов Российской Федерации Татьяна Проценко подчеркнула, что ценность очной ставки как раз состоит в психологическом воздействии. Оценивая доказательства, суд с большим доверием будет относиться к результатам очной ставки, нежели к результатам допроса. Очная ставка, производимая с использованием систем ВКС, по своей сути является дистанционным допросом, что, в свою очередь, будет вызывать нарушения [3].

Безусловно, нельзя не затронуть вопрос соблюдения прав и законных интересов участников уголовного судопроизводства. Невозможность узнать, что скрывается за объективами камер, затрудняет проведение следственных действий с использованием систем ВКС. Критикуя такой формат проведения, некоторые юристы-теоретики говорят о том, что видеозапись не позволит в полной мере оценить достоверность показаний. Данный тезис объясняется следующим образом: видеозапись может зафиксировать только то лицо, которое находится в зоне видимости камеры, а что происходит за объективами камер – никто не знает, и это вступает в противоречие с положениями ст. 11 УПК РФ. Поскольку никто не может определить, что скрывается за объективами камер, возникает возможность «подговорить» лицо, участвующее в следственном действии. Для решения обозначенной проблемы, по нашему мнению, перед началом действия в обязательном порядке лицо, в отношении которого оно проводится, должно показать помещение и все используемые технические устройства.

Результаты проведения следственного действия фиксируются в протоколе. При составлении этого документа обязательным условием является указание времени начала и окончания проводимого следственного действия. При использовании ВКС может возникнуть несоответствие часовых поясов, что, в свою очередь, будет нарушать положения ст. 164 УПК РФ [4, с. 343]. По нашему мнению, для решения данной проблемы на законодательном уровне необходимо закрепить перечень городов России с указанием часовых поясов и временного промежутка, с которого можно начинать и до истечения которого стоит завершить проведение следственных действий.

Кроме этого, каждое лицо, участвующее в проведении следственного действия, обязано поставить свою подпись, чтобы доказать факт достоверности происходящего и подтвердить согласие с указанной в процессуальном документе информацией.

При использовании ВКС такая возможность отсутствует. Анализируемая система проведения следственных действий предусматривает наличие подписей следователя или дознавателя, ответственных за проведение предварительного расследования, и следователя или дознавателя на территории, где находится лицо, участвующее в следственном действии, и подписи самого такого лица. Если одно из указанных лиц по какой-либо причине не поставит свою подпись, данное следственное действие будет расценено как недопустимое доказательство в соответствии со ст. 75 УПК РФ. При использовании ВКС обязательна видеозапись проводимого мероприятия (впоследствии видео будет приобщено к материалам уголовного дела). Однако сам факт наличия подобной видеозаписи нельзя считать полноценным доказательством, поэтому необходим протокол с подписями участвующих лиц. Чтобы протокол проведения следственного действия, совершенного с использованием ВКС, имел юридическую силу и мог быть приобщен к материалам уголовного дела, необходимо, по нашему мнению, ввести такой вид подписи, как электронная.

Основная проблема использования ВКС при проведении следственных действий, перечисленных в ст. 189.1 УПК РФ, напрямую связана с технической оснащенностью. В служебных кабинетах территориальных органов внутренних дел в большинстве случаев отсутствует соответствующая техническая возможность, а именно оснащение специальным оборудованием, позволяющим обеспечить эффективное взаимодействие между следователем-организатором, следователем, проводящим следственное действие, и участвующими лицами, соответственно. Считаем необходимым увеличить финансирование для обеспечения территориальных органов нужным оборудованием. Важно понимать, что наличие инновационных технологий позволит гарантировать качественное подключение, от которого, в свою очередь, зависит качество проводимого следственного действия.

Помимо технической оснащенности необходимо учитывать и наличие специальных знаний у сотрудников, производящих упомянутые следственные действия. Для повышения технической грамотности практических работников органов внутренних дел целесообразно проводить постоянные занятия, способствующие изучению, грамотному и эффективному использованию систем ВКС при проведении следственных действий.

Стоит отметить, что использование систем видео-конференц-связи имеет важное значение, способствует улучшению уголовного судопроизводства на досудебной стадии. При этом наличие имеющихся в уголовно-процессуальном законодательстве пробелов позволяет говорить о необходимости его совершенствования. Очевидно, что использование систем ВКС предоставляет ряд преимуществ по сравнению с применением традиционных способов проведения допроса, очной ставки и опознания, является значительным прогрессивным шагом, позволяющим разрешить имеющиеся проблемы.

Список библиографических ссылок

1. Долгинов С. Д. Технологии применения видеоконференцсвязи на предварительном следствии: проблемы сегодняшнего дня // Пермский юридический альманах. 2023. № 6. С. 470–485. URL: https://cyberleninka.ru/article/n/tehnologii-primeneniya-videokonferentssvyazi-na-predvaritelnom-sledstvii-problemy-segodnyashnego-dnya (дата обращения: 24.02.2025).

2. Пашутина О. С., Алымов Д. В. Очная ставка: проблемные аспекты уголовно-процессуального регулирования // Российский следователь. 2020. № 6. С. 13–16.

3. Стороженко А. Введенные в УПК нормы серьезно нарушают право на защиту // Адвокатская газета. 2022. № 2 (355) 16–31 января. URL: https://www.advgazeta.ru/novosti/vvedennye-v-upk-normy-serezno-narushayut-pravo-na-zashchitu / (дата обращения: 24.02.2025).

4. Проблемы проведения допроса путем использования систем видеоконференц-связи / Б. Б. Бидова, Ю. В. Быстрова, А. А. Комоско [и др.] // Право и государство: теория и практика. 2023. № 7 (223). С. 341–343. URL: https://cyberleninka.ru/article/n/problemy-provedeniya-doprosa-putem-ispolzovaniya-sistem-videokonferents-svyazi (дата обращения: 24.02.2025).

Александр Игоревич Трусов,
начальник кафедры уголовного процесса и криминалистики
Ставропольского филиала
Краснодарского университета МВД России,
кандидат юридических наук

СОВЕРШЕНСТВОВАНИЕ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА О ПРИМЕНЕНИИ ВИДЕО-КОНФЕРЕНЦ-СВЯЗИ НА СТАДИИ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

В настоящее время практическим работникам следствия (дознания) не хватает организационно-тактических рекомендаций по реализации на практике нормы ст. 189.1 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ), положения которой подвергаются обоснованной критике. Отсутствие этих рекомендаций вызывает определенные трудности в правоприменительной деятельности.

Мнения ученых-процессуалистов относительно совершенствования положений данной нормы расходятся.

Звучат предложения о расширении списка следственных действий, осуществляемых с использованием видео-конференц-связи (далее – ВКС) [1, с. 258]. Одни предлагают добавить в него освидетельствование, следственный эксперимент и проверку показаний на месте [2]. Ю. А. Цветков дополняет этот список выемкой и обыском [3], а П. Е. Власов – осмотром места происшествия с использованием БПЛА [4]. Другие выступают против применения ВКС, ссылаясь на «разную гносеологическую природу» некоторых следственных действий [5, с. 111]. Третьи видят возможность применения ВКС при осуществлении следственных действий, «объединенных методом расспроса» [6]. Е. Г. Кравец, Н. В. Шувалов и А. Н. Мартынов предлагают добавить к списку только освидетельствование как имеющее высокий коэффициент повторяемости в правоприменительной практике, а включение остальных юристы считают нецелесообразным по экономическим и правовым причинам [7].

П. А. Самсоновым обосновано расширение списка дистанционных следственных действий процессуальным действием – возможностью дистанционно признавать конкретное лицо потерпевшим [8]. Такое предложение заслуживает поддержки, так как подразумевает придание лицу конкретного статуса, без которого осуществить предусмотренные ст. 189.1 УПК РФ следственные действия не представляется возможным. Вместе с тем, по нашему мнению, не следует ограничиваться только лишь статусом потерпевшего, было бы правильным регламентировать аналогичные действия и в отношении других участников уголовного судопроизводства, таких как подозреваемый и обвиняемый (избрание некоторых мер пресечения, привлечение в качестве обвиняемого и предъявление обвинения), а также расширить рамки предложенных процессуальных действий, требующих ознакомления соответствующих лиц (например, ознакомление с назначением и заключением экспертизы, разрешение ходатайств, ознакомление с материалами уголовного дела), при обеспечении права на получение соответствующих копий. Для этого потребуется развитие отдельного направления: введение и использование цифровых форм процессуальных документов, формирование материалов уголовного дела в формате электронных документов [4].

Возможность применения ВКС также регламентируется ст. 164 и 166 УПК РФ [9], в которых отсутствуют требования к используемой инфраструктуре и программному обеспечению [10].

Еще в 2014 г. в деятельность МВД России был внедрен программно-аппаратный комплекс «СВКС» [11], входящий в электронный документооборот ИСОД МВД России. Комплекс позволяет выполнять требования ст. 161 УПК РФ на должном уровне. Он обеспечивает подключение к интегрированной мультисервисной телекоммуникационной системе (ИМТС), именуемой иногда внутриведомственным VPN. Система предоставляет необходимую степень защиты передаваемой информации подключенных пользователей, которые во время сеанса ВКС не подключены к Интернету, и действует при работе не только на стационарных компьютерах, но и в мобильных устройствах со специальными SIM-картами (планшетах) [12]. Именно поэтому применение общедоступных средств ВКС, не обеспечивающих должную защиту информации, по нашему мнению, недопустимо.

На сложности в реализации соответствующих изменений УПК РФ, связанные с недостаточной оснащенностью следственных органов необходимыми для ВКС техническими средствами, обращают внимание и другие авторы [13]. При этом законодателем не определен круг лиц, в отношении которых возможно применение новых технологий, однако анализ положений УПК РФ позволяет процессуалистам отнести к таким участникам подозреваемого, обвиняемого, свидетеля, потерпевшего, специалиста, эксперта, лицо, в отношении которого уголовное дело выделено в отдельное производство в связи с заключением с ним досудебного соглашения о сотрудничестве [14]. Некоторые ученые предлагают исключить из этого списка подозреваемого и обвиняемого: с ними необходимо проводить большое количество других следственных действий, не предусмотренных в формате ВКС [15, с. 101]. Другие говорят о необходимости включения в данный список тяжелобольных лиц и лиц с ограниченными возможностями здоровья, определения особенностей применения новых технологий в связи с их потенциальным участием [16]. Третьи считают нужным распространить применение технологий ВКС на всех субъектов уголовно-процессуальной деятельности, вне зависимости от процессуального статуса [17]. Последнюю точку зрения считаем самой взвешенной и не требующей дополнительного реформирования УПК РФ.

Таковыми участниками должны стать все субъекты уголовно-процессуальной деятельности, имеющие различного рода процессуальные статусы, а саму процедуру веб-конференции необходимо максимально приблизить к реальным процессуальным процедурам.

Проведенное нами исследование позволяет констатировать, что в условиях цифровизации общественных отношений системы видео-конференц-связи становятся востребованными в рамках уголовного судопроизводства, в том числе на стадии предварительного расследования.

Считаем необходимым выдвинуть следующие научно обоснованные предложения:

1. Внедрение видео-конференц-связи не требует пересмотра основополагающих принципов и правил производства предварительного расследования.

2. Использование систем видео-конференц-связи допустимо только на программно-аппаратных комплексах по типу СВКС, обеспечивающих необходимую степень защиты передаваемой информации подключенных пользователей.

3. Уголовно-процессуальные процедуры требуют совершенствования технологий видео-конференц-связи в части расширения количества подключаемых участни-

ков либо параллельного внедрения систем, предоставляющих веб-конференц-связь многочисленным участникам.

4. Возможности видео-конференц-связи должны быть доступны для всех участников уголовного судопроизводства.

5. Применение видео-конференц-связи допустимо при производстве не только допроса, очной ставки и опознания, но и других следственных и процессуальных действий, которые нуждаются в законодательном урегулировании, при обеспечении права на получение соответствующих копий.

Список библиографических ссылок

1. Пономаренко Ю. Н. Особенности проведения допроса, очной ставки, опознания путем использования систем видео-конференц-связи: актуальные проблемы и пути их решения // Вестник науки. 2022. № 6 (51). Т. 1. С. 257–262.

2. Щерба С. П., Архипова Е. А. Применение видео-конференц-связи в уголовном судопроизводстве России и зарубежных стран: опыт, проблемы, перспективы. М.: Юрлитинформ, 2016. 212 с.

3. Цветков Ю. А. Инквизиционный процесс: версия 2.0 (цифровая инквизиция) // Уголовное судопроизводство. 2023. № 1. С. 21–28.

4. Власов П. Е. Приоритетные направления цифровой трансформации уголовного судопроизводства // Российский следователь. 2023. № 6. С. 15–19.

5. Овчинникова О. В. Дистанционные следственные действия: современное состояние и перспективы // Юридическая наука и правоохранительная практика. 2019. № 1 (47). С. 108–116.

6. Семенцов В. А. Применение технологии видео-конференц-связи в судебном заседании и при производстве следственных действий // Библиотека криминалиста. Научный журнал. 2016. № 6 (29). С. 100–106.

7. Кравец Е. Г., Шувалов Н. В., Мартынов А. Н. Перспективы использования видео-конференц-связи при производстве следственных действий на досудебных стадиях уголовного судопроизводства // Юридическая наука и правоохранительная практика. 2017. № 4 (42). С. 175–181.

8. Самсонов П. А. Дистанционное участие потерпевшего в процессуальных действиях на стадии предварительного расследования // Актуальные проблемы российского права. 2023. № 5. С. 132–141.

9. Глимейда В. В. Проблема допустимости применения видео-конференц-связи при производстве следственных действий // Журнал юридических исследований. 2023. № 2. Т. 8. С. 116–124.

10. Валов С. В. Ресурсное обеспечение цифровой трансформации следственной деятельности // Российский следователь. 2023. № 3. С. 2–6.

11. Мещеряков В. В России работает «самая большая в мире» система видео-конференц-связи // Информационные технологии завтра: сайт. URL: https://www.cnews.ru/news/top/2026-03-18_v_rossii_rabotaet_samaya_bolshaya_v_mire_sistema?ysclid=mfpf8kma2h450398093 (дата обращения: 10.05.2024).

12. Шевырталов Е. П., Дерюгин Р. А. Организационно-тактические особенности проведения допроса с использованием систем видео-конференц-связи // Электронное приложение к «Российскому юридическому журналу». 2023. № 1. С. 45–50.

13. Сенокосов А. А. Пути совершенствования правовой регламентации оказания квалифицированной юридической помощи участникам уголовного судопроизводства

в условиях развития цифровых технологий // Актуальные проблемы российского права. 2023. № 8. С. 108–115.

14. Афанасьева С. И., Добровлянина О. В. О внедрении, развитии, усовершенствовании электронных способов собирания доказательственной информации по уголовным делам // Вестник Пермского университета. Юридические науки. 2023. № 2. С. 349–377.

15. Козловский П. В., Усольцева Д. Е. Теоретико-правовые аспекты использования средств видео-конференц-связи при производстве допроса в России и за рубежом // Вестник Сибирского института бизнеса и информационных технологий. 2022. Т. 11. № 3. С. 100–103.

16. Дударев В. А. Дистанционный допрос несовершеннолетних в зарубежных странах и Российской Федерации: проблемные вопросы // Международное уголовное право и международная юстиция. 2023. № 2. С. 18–22.

17. Гринь Д. С. Видео-конференц-связь в уголовном судопроизводстве: современное состояние и перспективы развития // Юридическая наука. 2020. № 5. С. 103–106.

Марина Николаевна Шарлова,
старший преподаватель кафедры административного права
и административной деятельности
Ставропольского филиала
Краснодарского университета МВД России

ВЛИЯНИЕ МИГРАЦИОННЫХ ПРОЦЕССОВ НА СОСТОЯНИЕ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ, В ТОМ ЧИСЛЕ С ИСПОЛЬЗОВАНИЕМ IT-ТЕХНОЛОГИЙ

Россия – миграционно привлекательная страна, традиционный рынок применения трудовых ресурсов из стран СНГ и дальнего зарубежья.

За последние несколько лет, по данным Федеральной пограничной службы ФСБ России, ежегодно в нашу страну с различными целями совершают поездки более 22 млн иностранных граждан и лиц без гражданства; некоторые из них находятся здесь незаконно [1].

Современная миграционная ситуация в России характеризуется присутствием большого числа иностранных граждан, не соблюдающих режим пребывания.

По данным Федеральной пограничной службы ФСБ России, за последние 5 лет количество нарушителей и незаконных мигрантов, задержанных на границе Российской Федерации, возросло почти в 10 раз.

Незаконной миграции из-за рубежа способствует ряд причин:

– использование поддельных документов;

– обстановка, сложившаяся на территории Украины и в новых субъектах Российской Федерации, а именно проведение специальной военной операции (далее – СВО).

Испытывая объективные и субъективные трудности, возникающие в процессе социальной адаптации в условиях иностранного государства, мигранты закономерно стремятся к сплочению с земляками, образуя этнические землячества или общины, в основном представляющие собой замкнутые социумы. В настоящее время в этнических общинах, помимо обособленности, наблюдается жесткая иерархичность, клановость, процветает круговая порука. Отмечаются попытки установления этническими криминальными структурами контроля за жизнью диаспор и общин.

Доля преступлений, совершенных иностранцами, в общем количестве преступлений в течение последних 10 лет оставалась относительно стабильной. Так, согласно официальным статистическим данным МВД России, количество преступлений, совершенных иностранными гражданами и лицами без гражданства, в отчетный период с января по октябрь 2024 г. сократилось на 2,6 %, число иностранных граждан, привлеченных к ответственности за совершение преступлений, снизилось на 3,8 %. В общем массиве предварительно расследованных преступлений противоправные деяния, совершенные иностранными гражданами, составили 4,3 %. Сократилось на 4,4 % количество совершенных иностранными гражданами тяжких и особо тяжких преступлений, в том числе убийств и покушений на убийство – на 4,3 %, против собственности – на 6,2 %, преступлений, связанных с незаконным оборотом наркотических средств, – на 18,1 % [2].

Особое внимание в настоящее время привлекают к себе незаконная миграция и экстремистские организации украинских спецслужб (далее – СБУ), которые вербуют мигрантов, управляют ими посредством запрещенных в России мессенджеров, обещают вознаграждение в виде криптовалюты.

Сейчас, в условиях СВО, украинские спецслужбы пытаются вести свою подрывную деятельность, не гнушаясь террористическими методами и не придавая значения возможности появления случайных жертв. Подобным образом был совершен ряд вероломных посягательств на жизнь общественных деятелей, журналистов, правоохранителей в разных субъектах Российской Федерации. Личное общение с исполнителями не требуется: все указания СБУ осуществляются дистанционно, с помощью информационно-коммуникационных технологий.

Так, например, в Санкт-Петербурге в результате теракта погиб военный корреспондент Владлен Татарский. Подготовкой к совершению преступления долгое время руководили с территории Украины. Следователи установили круг причастных, среди них – Дарья Трепова, уже представшая перед судом, а также Роман Попков и Юрий Денисов, живущие ныне в Киеве и сотрудничающие с беглым иноагентом, бывшим депутатом Госдумы, заочно арестованным в России Ильей Пономаревым, также проживающим на Украине. Пономареву заочно предъявлено обвинение. Попков, как установило следствие, познакомил Трепову с сотрудником СБУ. Передача последним заданий террористке осуществлялась в социальных сетях [3].

Другой пример – теракт в Нижегородской области, в результате которого был ранен Захар Прилепин, а водитель писателя погиб. В кратчайший срок после совершения преступления удалось установить и задержать подозреваемого Александра Пермякова, завербованного сотрудниками СБУ. По их заданию в августе 2022 г. он через Польшу и Эстонию прибыл в Россию и получил гражданство. В течение полугода выбирал место теракта. Необходимые денежные средства, пистолет, две противотанковые мины были переданы ему вербовщиками. Следствием обнаружены и осмотрены места хранения Пермяковым оружия и боеприпасов. В настоящее время продолжается установление соучастников этого преступления и всех его обстоятельств [4].

Расследуются и совершаемые при участии СБУ факты посягательств на жизнь правоохранителей и должностных лиц в новых регионах. Например, к длительным срокам лишения свободы приговорены граждане Украины Виталий Скакун и Юрий Доманчук, которые под руководством сотрудника СБУ совершили теракт, направленный против заместителя губернатора Херсонской области: чиновник был ранен, а его водитель погиб [5].

В большинстве подобных случаев четко выявляется миграционный след. Людей вводят в заблуждение и под различными предлогами, обещая вознаграждение, подталкивают к совершению противоправных действий. В условиях современности проще всего привлечь к этой деятельности мигрантов.

Особое внимание необходимо уделить выдаче иностранным гражданам сертификатов о владении русским языком, знании истории и основ законодательства Российской Федерации.

Отметим, что в 2021 г. произошли изменения в части проведения экзамена для получения сертификатов. Так, с 31 мая 2021 г. экзамены могут принимать только образовательные организации, входящие в официальный перечень, указанный в Постановлении Правительства Российской Федерации от 31 мая 2021 г. № 840 «Об утверждении требований к минимальному уровню знаний, необходимых для сдачи экзамена по русскому языку как иностранному, истории России и основам законодательства Российской Федерации, а также к уровню владения русским языком, знания истории России и основ законодательства Российской Федерации для целей приобретения гражданства Российской Федерации».

По данным Минобрнауки России, в период с 1 января 2020 г. по 30 января 2023 г. экзамен сдали более 4 млн иностранных граждан. Около 85 % экзаменуемых прошли испытание успешно и получили сертификаты [6].

На первый взгляд, эти изменения должны были ужесточить порядок получения сертификатов, и количество случаев получения сертификатов лицами, не владеющими русским языком, должно было уменьшиться, однако этого не произошло: как показывает практика общения с гражданами из стран ближнего зарубежья, многие из них не знают русского языка. В основном это приезжие из Средней Азии, которые сезонно работают в субъектах Российской Федерации. На работе они общаются с земляками на родном языке. Даже представители организаций, помогающих этим людям с оформлением документов, разговаривают с ними на их родном, а не на государственном национальном языке. Как правило, всегда есть выходец из страны ближнего зарубежья, уже обосновавшийся в субъекте Российской Федерации, интегрировавшийся в общество и теперь помогающий своим землякам. То же происходит и с гражданами из дальнего зарубежья (например, из Вьетнама, Китая).

Говоря об актуальной проблеме, связанной с миграцией, отметим, что при рассмотрении заявлений, сообщений сотрудники органов внутренних дел (далее – ОВД) вызывают мигрантов для получения какой-либо дополнительной информации, какого-либо объяснения, и тут возникает проблема в общении и понимании.

Все это создает сложности в работе с мигрантами. Некоторые из них негативно воспринимают тот факт, что им необходимо знать русский язык, не понимают, для чего его нужно знать, если есть родственник, который им владеет и который при необходимости поможет. Возникают вопросы: как можно взаимодействовать с человеком, не знающим русский язык, как брать объяснение от человека, не способного его самостоятельно прочитать, как можно принимать те же заявления о выдаче патента, разрешения на временное проживание, получении вида на жительство, если документы приезжающим собирают организации, а сами мигранты не могут прочитать собственное заявление.

Постановлением Правительства Российской Федерации от 31 мая 2021 г. № 824 утверждено Положение о проведении экзамена по русскому языку как иностранному, истории России и основам законодательства Российской Федерации, в котором определен минимальный набор требований для получения иностранцами сертификата. Так, к примеру, иностранцы должны уметь читать небольшие по объему тексты рекламного и информационного характера (например, объявления, вывески, надписи, указатели), определять тему текста, понимать содержащуюся в нем основную и дополнительную информацию, актуальную для социально-бытовой, социально-культурной и официально-деловой сфер общения. Требуется также умение заполнять анкеты, бланки, писать заявления (например, о приеме на работу, о приеме ребенка в школу, о выдаче патента, разрешения на временное проживание и вида на жительство в Российской Федерации), понимать на слух основное содержание монолога и диалога в речевых ситуациях, характерных для социально-бытовой, официально-деловой, профессиональной и социально-культурной сфер общения, участвовать в диалоге. Получается, что у гражданина, имеющего на руках сертификат, не должно возникать проблем с заполнением собственного заявления и с предоставлением (при необходимости) пояснений относительно информации, указанной в его же заявлении.

В интервьюировании сотрудников подразделений по вопросам миграции было установлено, что 80 % трудящихся-мигрантов, получивших патент, просто не имеют минимальных знаний по русскому языку.

В целях локализации данных негативных тенденций в настоящее время ОВД должны приниматься превентивные меры, позволяющие увеличить количество расследованных преступлений, совершенных в сфере IT-технологий и связанных с незаконной миграцией, по сравнению с аналогичным периодом прошлого года.

На данный момент острота проблемы незаконной миграции в России, безусловно, сохраняется, но очевидно и определенное улучшение ситуации, ставшее следствием принимаемых государством мер, в том числе – на законодательном уровне. Поскольку эта проблема давно приобрела общемировой характер, необходимо объединение усилий заинтересованных государств в вопросах укрепления соответствующих правовых механизмов и углубления международных контактов в этой сфере.

Список библиографических ссылок

1. Более 15 млн иностранцев посетили РФ в 2023 году // РОСМИГРАНТ: офиц. сайт. URL: https://росмигрант.рф/press-center/news/novosti/bolee-15-mln-inostrantsev-posetili-rf-v-2023-godu (дата обращения: 15.01.2025).

2. Аналитическая справка о результатах деятельности подразделений по вопросам миграции территориальных органов МВД России за январь–октябрь 2024 года // МВД России: офиц. сайт. URL: https://мвд.рф/dejatelnost/statistics/migracionnaya/item/57172708 (дата обращения: 19.02.2025).

3. Дело о теракте в петербургском кафе, где погиб военкор Владлен Татарский // РИА НОВОСТИ: офиц. сайт. URL: https://ria.ru/20240125/terakt-1923283743 (дата обращения: 19.02.2025).

4. Покушение на Захара Прилепина // Википедия: офиц. сайт. URL: https://ru.wikipedia.org/wiki/Покушение_на_ЗахараПрилепина (дата обращения: 01.03.2025).

5. На Херсонщине считают, что покушение на замглавы региона совершили «террористы» Киева // ТАСС: офиц. сайт. URL: https://tass.ru/politika/16573973?ysclid=m7xcvf1w5b544643 334 (дата обращения: 01.03.2025).

6. Минобрнауки России: офиц. сайт. URL: https://minobrnauki.gov.ru/ (дата обращения: 01.03.2025).

Научное издание

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ В РОССИИ

Сборник научных трудов

Редактор *А. Н. Гайворонская-Кантомирова*
Компьютерная верстка *Н. А. Доненко*
Дизайн обложки *Н. А. Доненко*

Волгоградская академия МВД России.
400075, Волгоград, ул. Историческая, 130.

Редакционно-издательский отдел.
400005, Волгоград, ул. Коммунистическая, 36.

Подписано к использованию 30.09.2025. Объем 0,8 Мб.
Тираж 10 экз. Заказ 57.

ОПиОП РИО ВА МВД России. 400005, Волгоград, ул. Коммунистическая, 36.