Федеральное государственное казенное образовательное учреждение высшего образования «Сибирский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра уголовного права и криминологии

Специальность 40.05.01 Правовое обеспечение национальной безопасности,
специализация № 1 «Уголовно-правовая»
(узкая специализация – предварительное следствие
в органах внутренних дел)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:

КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ И ПРОФИЛАКТИКА

Выполнил:
Слушатель группы НБ 1802
младший лейтенант полиции
Тамалинцева Ульяна Дмитриевна

Руководитель:
Начальник кафедры уголовного права
и криминологии
кандидат юридических наук, доцент
полковник полиции
Мальков Сергей Михайлович

Дата защиты:
«22» 06 2023 г.

Оценка: хорошо

Председатель ГЭК
полковник юстиции _____ И.А. Юдаева
(специальное звание) (подпись) (инициалы, фамилия)

Красноярск 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы выпускной квалификационной работы

Обеспечение национальной безопасности Российской Федерации в Стратегии национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02 июля 2021 г. №400, названо в числе основных направлений и приоритетов Российской Федерации, а эффективные результаты этой деятельности – залог динамичного развития и стабильности государства. Важнейшим направлением в обеспечении национальной безопасности является кибербезопасность. Так в соответствии со ст. 3 Федерального закона от 27 июля 2006 №149-ФЗ «Об информатизации, информационных технологиях и защите информации» одним из принципов реализации информационных технологий является обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации.

Проблема борьбы с киберпреступностью весьма многогранна, она включает в себя широкий круг правовых, криминологических, социологических, психологических и других аспектов. Данная группа преступлений в криминологическом плане исследуется сравнительно недавно и связана с интенсивным развитием и эксплуатацией информационного, в том числе и киберпространства.

В связи с развитием информационных технологий четко сформировалось явление, состоящее в коренном изменении общественных отношений,

выражающемся в изменении их проявления в объективной действительности. Обращаясь к самой сущности отношений между людьми, мы можем констатировать тот факт, что в основе таких отношений лежит процесс передачи информации того или иного содержания. В свою очередь, современные технологии коренным образом преобразили указанный процесс передачи. Результатом преображения стало исключение из процесса информационного обмена такой характерной черты как непосредственность взаимодействия между сторонами передачи информации. В современном мире информация носит оперативный характер, что выражается в возможности её передачи за доли секунды в любую точку мира, в которой имеется техническая возможность такой передачи.

По официальным статистическим данным Минкомсвязи России, плотность абонентских устройств мобильной связи в России на 100 человек населения составляет 196,9 абонентских устройств, число активных абонентов мобильной связи, использующих услуги доступа в Интернет, составляет 131,4 миллиона человек. 61 % населения России по состоянию на 2022 год являются активными пользователями информационно-телекоммуникационной сети «Интернет»; в предпринимательском секторе 27 % используют возможности «облачных» хранилищ информации[1]. Указанные данные свидетельствуют лишь об одном – информация в подавляющем своем большинстве передается посредством использования современных коммуникационных технологий. Такое положение вещей не оставляет в стороне и процесс видоизменения такого социального явления как преступность, в котором, прежде всего, изменяются способы совершения преступлений и механизмы следообразования.

Особенно ярко такие изменения проявляются по уголовным делам, связанным компьютерными преступлениями, которые в последние годы приоб-

[1] Информационное общество. Оперативная информация [Электронный ресурс] URL: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innovations/it_technology/ (дата обращения: 28.01.2023 г.)

ретают все новые проявления и формы, что также будет являться предметом исследования, так как по сей день не выработана классификация компьютерных преступлений в криминалистической науке. Изменение указанных элементов вызывает объективную необходимость соответствующего преобразования процесса выявления и предупреждения данных категорий преступлений.

Успешное противодействие киберпреступлениям немыслимо без глубокого криминологического анализа понятия, причин, личности преступника, а также особенностей криминологической профилактика. Таким образом, представляется актуальным проведение соответствующего криминологического исследования по данной тематике.

Цель и задачи выпускной квалификационной работы

Целью работы является исследование теоретических и прикладных вопросов, связанных криминологической профилактикой киберпреступлений.

Задачами выпускной квалификационной работы является:

1. Рассмотрение понятия киберпреступности.
2. Анализ классификации киберпреступлений.
3. Выявление причин киберпреступности.
4. Характеристика личности лица, совершающего киберпреступления.
5. Формулирование типологии киберпреступников.
6. Анализ понятия, объектов и субъектов профилактики киберпреступности.
7. Анализ общекриминалогической профилактики киберпреступности.
8. Исследовать вопросы специально-криминологической профилактики киберпреступности.

Объект и предмет выпускной квалификационной работы

Объектом исследования являются общественные отношения, возникающие при осуществлении криминологической профилактики киберпреступности.

Предмет исследования включает в себя законодательство, отдельные доктринальные позиции относительно детерминации и противодействия киберпреступности, закономерности и особенности криминологического предупреждения киберпреступлений,

Степень научной разработанности проблемы

В становление и развитие системы мер профилактики киберпреступности внесли определенный вклад многие авторы. Вместе с тем, ранее проведенные исследования по данной теме носят фрагментарный характер и недостаточно для формулирования наиболее актуальных направлений противодействия киберпреступности, проблематика рассматриваемой темы существует и требует дальнейшего исследования.

Значение разработки для теории и практики деятельности органов внутренних дел и иных правоохранительных органов

Проведенное исследование позволило сформулировать выводы и рекомендации по выявлению и нейтрализации детерминантов киберпреступности. Сформулированные в исследовании предложения могут быть использованы в практической деятельности органов внутренних дел, а именно для подразделений, которые занимаются раскрытием и расследованием киберпреступлений (отдел-К, следственные подразделений по расследованию дистанционных преступлений, оперативные подразделения по расследованию дистанционных преступлений и т.д.).

Теоретическую основу исследования составили основные положения криминологии, а также относящиеся к объекту исследования труды в области криминологии и уголовного права. Криминологические и отдельные криминалистические аспекты противодействия и расследования компьютерных преступлений анализировались в работах П. В. Агапова, В. А. Бессонова, В.

Б. Вехова, А. Г. Волеводза, А. С. Егорашева, А. Н. Караханьяна, В. Е. Козлова, В. В. Крылова, В. В. Меркурьева, В. С. Овчинского, А. Л. Осипенко, А. Э. Побегайло, Н. С. Полевого, Л. Н. Соловьева, С. Е. Спириной, Е. В. Старостиной, Л. А. Сударевой, Н. Г. Шурухнова и других ученых.

Нормативную основу исследования составили: нормы Федерального и регионального законодательства, а также нормативные акты ведомственного уровня, концепции и иные официальные документы. В частности, Конституция Российской Федерации, Уголовный Кодекс Российской Федерации, Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет" и т.д.

Методологическую основу исследования составляет метод познания общественных процессов и правовых явлений. В работе применялись следующие методы: статистический, документальный, догматический (юридический) и системно-структурный.

Эмпирическую основу исследования составили статистические данные о состоянии и динамике киберпреступлений с 2018 по 2022 годы.

В работе использованы опубликованные данные исследований, проведенных другими авторами.

Структура работы определена целями и задачами исследования**.** Работа состоит из введения, двух глав, объединяющих в себя 6 (шесть) параграфов, заключения и списка использованной литературы.

ГЛАВА 1. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПНОСТИ

1.1. Понятие киберпреступности и криминологическая классификация киберпреступлений

Вначале обратимся к статистическим показателям киберпреступности. Количество зарегистрированных киберпреступлений в 2022 г. увеличилось на 0,8 % в сравнении с 2021 годом и составил 522 065 преступлений. Отмечается рост уровня киберпреступности: в 2018 году уровень киберпреступности составлял 118,9 преступления на 100 тысяч населения, в 2019 г. соответственно – 200,6, в 2020 г. отмечается резкий рост уровня преступности до 347,8, в 2021 г. – 352,9, в 2022 году уровень преступности составил 358,7 преступлений на 100 тысяч населения.

Отмечается значительная доля киберпреступности в общей структуре преступности: в 2021 году доля киберпреступности составляла 25,8 %, а в 2022 году – 26,5 %.

Существенно увеличился ущерб от IT преступлений и составил 91 041 183 тысяч рублей.

В 2022 году рост числа киберпреступлений наблюдался в Южном (2,8%), Центральном (2,1 %), Приволжском (1,3 %), Северо-Кавказском (7,8 %) федеральных округах. Максимальный рост киберпреступлений отмечается в Республике Северная Осетия (2 068; 47,8%), Тверской области (5 332; 28 %), Чукотском АО (213; 36 %), Рязанской области (2 245; 20,8 %), Республике Крым (4 893; 18,3 %), Московской области (15 061; 16,1 %), г. Севастополь

(1 509; 14,8 %). В 17 % субъектов Федерации зарегистрировано более 50 % всех киберпреступлений, совершенных в Российской Федерации.

Более половины всех зарегистрированных киберпреступлений (52,1 %) относится к категории тяжких и особо тяжких преступлений (в 2022 г. - 272 233 преступлений).

В структуре киберпреступности преобладают мошеннические действия (47,88 %), кражи (21,75 %), незаконный оборот наркотиков (11,92 %).

К наиболее распространенным способам совершения киберпреступлений относятся: с использованием телекоммуникационной сети «Интернет» (всего в 2022 г. – 381 112), при помощи средств мобильной связи (212 963), расчетных (пластиковых) карт (всего 127 149 преступлений) [1].

Глобальные процессы, происходящие в политике, экономике, науке и технике оказали существенное влияние на все сферы жизни современного общества и отдельного человека в нём, привели к серьёзным изменениям или возникновению абсолютно новых феноменов.

Киберпреступность нуждается в формулировании ее понятия и классификации, поскольку XXI век характеризуется быстрыми темпами развиваются компьютерные технологии. Однако все эти достижения имеют свою «оборотную» сторону, а именно - компьютерную преступность. Весь спектр преступных действий в сфере информационных технологий, будь то преступления, которые совершенны при помощи компьютеров, или те, предметом которых стали сами компьютеры, компьютерные сети и хранящаяся в них информация охватываются понятием «интернет-преступление» или «киберпреступление». «Компьютерное преступление» – это только то преступление, которое посягает на безопасное функционирование компьютеров и компью-

[1] Комплексный анализ состояния преступности в Российской Федерации по итогам 2022 года и ожидаемые тенденции ее развития / М.В. Гончарова, С.А. Невский, М.М. Бабаев, Р.В. Черкасов, Е.Б. Аблиязова, Е.М. Тимошина, Г.В. Коимшиди, Г.Э. Бицадзе – М.: ФГКУ «ВНИИ МВД России», 2023. С. 63-69.

терных сетей, а также на обрабатываемые ими данные[1]. Вместе с тем стоит отметить, что указанное понятие не является до конца верным и характеризует лишь одну сторону компьютерных преступлений.

На сегодняшний день четкой позиции относительного того, что следует понимать под компьютерной преступностью, в научном сообществе нет, и до сих пор ведутся многочисленные дискуссии о содержании и значении данного юридического понятия[2].

Одни авторы полагают, что компьютерная преступность — это совокупность преступлений, при совершении которых предметом преступных посягательств выступает компьютерная информация, и отождествляют при этом понятия компьютерного преступления и преступления в сфере компьютерной информации[3]. В указанном понятии, по нашему мнению, довольно узко представлен предмет преступного посягательства, так как компьютерные преступления могут ни только посягать на компьютерную информацию, но и совершать другие преступления с использованием электронных носителей информации и информационно-телекоммуникационной сети «Интернет».

Т.М. Лопатина считает, что под компьютерной преступностью следует понимать совокупность совершенных на определенной территории за конкретный период преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений, совершенных с использованием компьютера в целях извлечения материальной

---

[1] Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. 2016 № 1 (35). С. 22

[2] Евдокимов К.Н. Политические факторы компьютерной преступности в России // Информационное право. 2015. № 1. С. 41–47.; Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. М., 2015. С. 29.; Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами // Право и кибербезопасность. 2014. № 2. С. 27–32. и др.

[3] . Криминология: учебник / под общ. ред. А.И. Долговой. 4-е изд., перераб. и доп. М., 2013. С. 544.

выгоды или иной личной заинтересованности[1]. Указанное понятие является более точным и охватывает большое количество преступлений.

Д.В. Добровольский определяет компьютерную преступность как совокупность всех преступлений в сфере информационных технологий, а не только общественно опасных деяний, предметом которых является компьютерная информация[2].

По мнению А.А. Жмыхова, компьютерная преступность — это совокупность преступлений, совершаемых с помощью компьютерной системы или сети, в рамках компьютерной системы или сети и против компьютерной системы или сети. Таким образом, он относит к компьютерным преступлениям не только преступления в сфере компьютерной информации, но и преступления, связанные с компьютерами, т.е. такие традиционные по характеру преступные деяния, совершенные с помощью вычислительной техники, как кража, мошенничество, причинение вреда и др.[3]

В ряде научных работ встречается упоминание о киберпреступности — юридическом понятии, которое часто употребляется в научном обороте за рубежом и наиболее полно, по мнению авторов данных работ, отражает преступные деяния в сфере компьютерной информации, а также преступления, совершенные с помощью компьютерных устройств, информационно-телекоммуникационных сетей и информационных технологий[4]. Такой подход предполагает, что компьютерная преступность является только частью киберпреступности как более широкого понятия.

---

[1] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дисс. ... д-ра юрид. наук. М., 2007. С. 39.

[2] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дисс. … канд. юрид. наук. М., 2005. С. 49.

[3] Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дисс. … канд. юрид. наук. М., 2003. С. 13.

[4] Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дисс. … канд. юрид. наук. М., 2013. С. 14.

Отдельные ученые в своих работах отождествляют понятия преступности в Интернете, киберпреступности, компьютерной преступности[1].

Еще один подход предполагает параллельное существование понятий интернет-преступности и компьютерной преступности как части и целого. По мнению Р.И. Дремлюги не каждое преступление в сфере компьютерной информации представляет собой интернет-преступление, в то же время такие традиционные преступления, как мошенничество, кража, вымогательство и др., совершенные посредством сети Интернет, — это интернет-преступления. Причем их последствия не обязательно должны наступать в сети Интернет[2]. Полагаем, что данная точка зрения верна и понятие компьютерной преступности охватывает более широкий круг отношений и в том числе включает в себя проявления интернет-преступности.

С учетом описанных выше подходов к пониманию компьютерной преступности полагаем целесообразным рассматривать данное понятие в узком и широком смысле.

В узком смысле, по мнению авторов, компьютерная преступность представляет собой совокупность преступлений, при совершении которых в качестве основного объекта выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом являются компьютерная информация, средства ее хранения, обработки, передачи и защиты, информационно-телекоммуникационные сети.

Компьютерная преступность в широком смысле — это совокупность преступлений, при совершении которых объектом выступают любые общественные отношения в сфере информационных технологий и безопасного функционирования компьютерной информации. При этом компьютерная информация, средства ее создания, хранения, обработки и передачи (компьютеры, смартфоны, кассовые аппараты, банкоматы, платежные терминалы и

[1] Рассолов И.М. Право и Интернет. Теоретические проблемы. М., 2003. С. 255.
[2] Дремлюга Р.И. Интернет-преступность. Владивосток, 2008. С. 44.

иные компьютерные устройства), информационно-телекоммуникационные сети не только являются предметом преступного деяния, но и используются в качестве средства и орудия совершения преступления.

Таким образом, понятие компьютерной преступности в узком смысле охватывает преступления в сфере компьютерной информации, уголовная ответственность за которые предусмотрена в гл. 28 Уголовного кодекса Российской Федерации, а в широком смысле включает в себя понятия киберпреступности, интернет-преступности, преступности в сфере компьютерной информации, преступности в сфере информационных технологий. Представляется, что такой подход к пониманию компьютерной преступности позволит оценить всю сложность, многообразие, разноуровневность рассматриваемого криминального явления и найти определенный баланс среди существующих научных позиций. И именно данный подход будет использоваться в рамках исследования.

Исследование научной литературы по рассматриваемой теме также показывает неоднозначность мнений ученых относительно структуры компьютерной преступности в России. Например, Д.К. Чирков и А.Ж. Саркисян в структуре компьютерной преступности выделяют только те преступные деяния, которые учитываются ГИАЦ МВД России как преступления, совершенные в сфере телекоммуникаций и компьютерной информации[1]. Указанный подход может иметь право на существование, вместе с тем он не может считаться верным с точки зрения криминалистической характеристики компьютерных преступлений, поскольку отражает лишь усеченную группу зарегистрированных преступлений с определенным, а также напрямую зависит от правоприменительной практики выставления статистических карточек.

По мнению М.Б. Эмирова, А.Д. Саидова, Д.А. Рагимханова, к наиболее распространенным видам преступлений в глобальных компьютерных сетях

[1] Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. 2013. № 3. С. 219-226.

можно отнести промышленный шпионаж, саботаж, вандализм, спуфинг (взлом паролей), мошенничество[1].

Другие авторы исходят из сложной структуры компьютерной преступности и рассматривают входящие в нее преступные деяния по нескольким критериям: объект, предмет посягательства, способ совершения и т.п.[2] Например, по объекту посягательства выделяются следующие группы компьютерных преступлений: преступления против конфиденциальности, целостности, доступности компьютерных данных и компьютерных сетей; экономические компьютерные преступления; компьютерные преступления против личных прав и неприкосновенности частной сферы; компьютерные преступления против общественных и государственных интересов[3].

По предмету преступного посягательства преступления подразделяются на преступления, имеющие материальный предмет посягательства, и преступления, не имеющие такового. По численности субъектов преступления – совершённые одним лицом; группой лиц.

По мнению авторов, для оценки структуры компьютерной преступности в России предпочтительней использовать криминологическую классификацию и статистику совершенных компьютерных преступлений, применяемые правоохранительными органами, т.е. «нормативный» подход. Это обусловлено тем, что существующая методика учета зарегистрированных, расследованных, приостановленных и прекращенных уголовных дел по преступлениям данного вида уже апробирована временем, а уголовная статистика складывается из ежедневно поступающих данных от территориальных органов ФСБ, МВД, Следственного комитета Российской Федерации. В силу этого правоохранительные органы обладают большим объемом аналитической

[1] Эмиров М.Б., Саидов А.Д., Рагимханов Д.А. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник Дагестанского государственного университета. 2011. № 2. С. 63–66.

[2] Номоконов В.А., Тропина Т.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 45–55.

[3] Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. 2013. № 5 (10). С. 148–160.

информации о структуре и масштабах компьютерной преступности в России, чем экспертное или научное сообщество, что не умаляет роли последних в исследовании данного криминального явления[1].

В этой связи можно представить следующую криминологическую классификацию компьютерных преступлений:

1. Преступления в области компьютерной информации: (незаконный доступ к компьютерной информации (ст.272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ).

2. Преступления, совершаемые с применением компьютера:

- Компьютерные преступления против личности (ст. клевета (ст. 128.1 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), отказ в предоставлении гражданину информации (ст. 140 УК РФ), нарушения избирательных прав или работы избирательных комиссий (ст. 141, 141.1, 142, 142.1 УК РФ), воспрепятствование законной профессиональной деятельности журналистов (ст. 144 УК РФ).

- Компьютерные преступления экономического характера (кража, мошенничество, хищение предметов, которые имеют особую ценность, умышленное уничтожение или повреждение имущества, заведомо ложная реклама, неправомерное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, изготовление и сбыт поддельных кредитных карт, незаконный экспорт технологий, научно-технической информации (ст. 158, 159, 164, 167, 182, 183, 187, 189 УК РФ).

[1] Скляров С.В., Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 2. С. 322–330.

• Компьютерные преступления против общественной безопасности и общественного порядка (заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей, общества (ст. 237 УК РФ).

• Компьютерные преступления против государственной власти (государственная измена (ст. 275 УК РФ), шпионаж (ст. 276 УК РФ), разглашение государственной тайны (ст. 283 УК РФ).

Д.А. Илюшин выделяет следующие виды киберпреступлений:

1. Неправомерное подключение к сети Интернет;

2. Создание, использование и распространение вредоносных программ;

3. Незаконное изготовление, хранение, распространение, рекламирование и (или) публичная демонстрация информации, запрещённой к свободному обороту, совершённое с использованием сети Интернет;

4. Нарушение авторских и смежных прав, а также незаконное использование чужого товарного знака, совершённые с использованием сети Интернет;

5. Компьютерное мошенничество;

6. Хищение электронных реквизитов и сбыт поддельных кредитных либо расчётных карт;

7. Незаконное предпринимательство в сфере предоставления услуг Интернет;

8. Вымогательство, совершённое с использованием сети Интернет;

9. Кибертерроризм[1].

В.А. Мещеряков классифицирует преступления в сфере компьютерной информации по объекту преступного посягательства – компьютерной информаций. На основе этого критерия выделяет следующие виды:

1. Уничтожение (разрушение) компьютерной информации.

[1] Илюшин, Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дисс. … канд. юрид. наук. Волгоград, 2008. С. 155.

2. Неправомерное завладение компьютерной информацией или нарушение исключительного права на её использование:

- Неправомерное завладение алгоритмом (методом) преобразования компьютерной информации;

- Неправомерное завладение совокупностью сведений, документов – нарушение исключительного права владения;

- Неправомерное завладение компьютерной информацией как товаром.

3. Действия или бездействие по созданию компьютерной информации с заданными свойствами:

- Распространение по телекоммуникационным каналам информационно-вычислительных сетей компьютерной информации, наносящей ущерб абонентам;

- Разработка и распространение компьютерных вирусов и прочих вредоносных программ для ЭВМ.

4. Неправомерная модификация компьютерной информации:

- Неправомерная модификация компьютерной информации как совокупности фактов, сведений;

- Неправомерная модификация компьютерной информации как алгоритма;

- Неправомерная модификация компьютерной информации как товара с целью воспользоваться её полезными свойствами[1].

В.Б. Веховым компьютерные преступления следует классифицировать по роли компьютерной техники в механизме преступного деяния:

1) во-первых, когда компьютерная техника выступает в роли предмета посягательства;

2) во-вторых, когда компьютерная техника выступает в роли орудия и средства совершения преступления. В этом случае предметом посягательства является информация, а орудием выступает компьютерная техника[1].

[1] Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста: научный журнал. 2013. № 5 (10). С. 265 - 270

Важно отметить, что классифицировать компьютерные преступления возможно лишь согласовав различного рода основания. Например, все без исключения компьютерные преступления можно разбить на две большие категории:

1.Преступления, которые непосредственно связаны с вмешательством в работу компьютеров.

2.Преступления, использующие компьютеры как необходимые технические средства.

В научном сообществе киберпреступления, в широком смысле, обозначены как общественно опасные деяния, посягающие, помимо компьютерных систем, на иные объекты, к основным из которых относятся: национальная и мировая безопасность (кибертерроризм), имущество, имущественные права индивидов и их коллективных образований (это и кражи, и мошенничество, совершенные посредством компьютерных систем или в киберпространстве, а также посягательства на авторские права (плагиат и киберпиратство), на личную безопасность (явления кибербуллинга и секстинга, груминга и троллинга) и пр.[2]

Характерными признаками киберпреступлений являются не только общественная опасность, но и оперативность совершения деяния, удаленность, а также масштабность и высокая анонимность, отражающаяся не только в сложности обнаружения виновного, но и в вероятности предоставить информацию потребителю, не соответствующую действительности. Такой признак киберпреступности, как самодостаточность, облегчает совершение и сокрытие посягательства, а признак виртуальности характеризует место деяния в качестве идеальной не опознанной с точностью среды для «трансформации» личности преступника, перевоплощения и корректирования характе-

---

[1] Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского М., 1996. С. 27.

[2] Мирончик А.С., Суслопаров А.В. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации // Юридические исследования. 2019. № 9. С. 17.

ристик (внешнего вида и пр.). В связи с тем, что определенная часть киберпреступлений остается вне поля зрения правоохранительных органов, данным посягательствам свойственен признак латентности, характеризующийся как объективное социально-юридическое явление, которому свойственны отдельные и качественные, и количественные особенности. Латентная киберпреступность, соответственно, – комплекс деяний, совершенных с применением информационно-телекоммуникационных технологий, которые признаны не выявленными и (либо) не учтенными национальными правоохранительными органами на определенной территории в соответствующий период времени[1].

Актуальность киберугроз, обусловленная ростом киберпреступности как нового общественно опасного деяния, активизирующегося на мировом и национальном уровне[2], повлияла на эволюцию международного сотрудничества в обозначенном направлении. Российская Федерация является участницей Конвенции о преступности в сфере компьютерной информации[3], выступает инициатором принятия на уровне Организации Объединенных Наций новой Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях[4], проект которой в рам-

[1] Бойко О.А., Унукович А.С. Детерминанты латентных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Юридический вестник Самарского университета. 2020. № 6 (3). С. 53–59.

[2] Егоров И. Россия внесла в ООН первый проект Конвенции по борьбе с киберпреступностью // Российская газета. 2021. № 168 (8519) [Электронный ресурс] // Официальный сайт Российской газеты. URL: https://rg.ru/2021/07/27/rossiia-vnesla-v-oon-perv yj-proekt-konvencii-po-borbe-s-kiberprestupnostiu.html (дата обращения: 22.01.2023).

[3] Конвенция о преступности в сфере компьютерной информации (ETS № 185) (г. Будапешт, 23.11.2001) // СПС «Гарант».

[4] Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (проект от 29.06.2021). URL: https://www. kommersant.ru/docs/2021/RF_28_July_2021_-_R.pdf (дата обращения: 22.01.2023).

ках Резолюции ООН[1] был направлен в Совет Безопасности ООН (июнь 2021 г.).

Таким образом подводя итоги рассмотрению данного вопроса отметим, что киберпреступления на сегодняшний день представляют большую общественную опасность. Рассмотрев отдельные виды киберпреступлений можно прийти к выводу о том, что они это общественно опасное деяние, совершенное в электронной сфере посредством применения информационно-коммуникационных технологий, ресурсов компьютерной информации, т. е. компьютерной системы либо сети, непосредственно – в названной системе либо в сети, либо против названных объектов, посягающее в т. ч. на национальную и мировую безопасность (кибертерроризм и пр.), имущество, имущественные права (кражи, мошенничество в киберпространстве), личную безопасность (кибербуллинг, секстинг, груминг, троллинг и пр.), интеллектуальную собственность (плагиат и киберпиратство) и пр. Характерные признаки киберпреступности: общественная опасность, латентность, оперативность, удаленность, масштабность и высокая анонимность, самодостаточность, виртуальность.

1.2. Причины киберпреступности

Сегодняшнее положение вещей таково, что современная преступность представляет собой условную «лакмусовую бумажку», которая отражает состояние общественных отношений, развитие технологий и т.д. С развитием телекоммуникационных технологий покупка-продажа наркотиков стала быть «бесконтактной», что создало достаточно серьезные сложности для правоох-

[1] Резолюция Генеральной Ассамблеи ООН от 27 декабря 2019 г. № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». URL: https://www. un.org/ru/ga/ (дата обращения: 22.01.2023)

ранительных органов в силу того, что возникла потребность разработки и использования новых методик раскрытия и расследования преступлений.

Проблема причин преступности является одной из центральных в науке криминологии и предупреждении правонарушений. Причинный комплекс преступности включает ее причины и условия, которые в совокупности составляют факторы преступности. Причины – это социально-психологические детерминанты, которые непосредственно порождают, воспроизводят преступность и преступления как свое закономерное следствие; условия – это такие социальные явления, которые сами не порождают преступность и преступления, а способствуют, облегчают, интенсифицируют формирование и действие причины[1].

Анализ криминологической науки свидетельствует о выделении причин, способствующих совершению рассматриваемых видов преступлений: недостаточная защита средств электронной почты; небрежность в работе пользователей информационно-коммуникационных технологий (ИКТ); недостаточная защита при использовании ИКТ в конкретных технологических процессах и операциях и т. д.[2] Кроме субъективных причин, по нашему мнению, наиболее типичными причинами и условиями совершения преступлений в сфере информационных технологий и безопасности на современном этапе являются:

– рост числа ИКТ и, как следствие, увеличение объемов информации, обрабатываемой и хранимой в ИКТ;

– недостаточность мер по защите ИКТ, систем ИКТ и их сетей;

– недостаточность защиты программного обеспечения;

– рост информационного обмена через мировые информационные сети, в первую очередь, посредством социальных сетей;

---

[1] Гладких В.И. Криминология: учебник (бакалавриат и магистратура). М., 2019. С. 167.

[2] Расулиев А. Киберпреступность: причины и условия, личность преступника // Вестник юридических наук. 2020. № 4. С. 12.

– отсутствие, несовершенство или отступление от правил эксплуатации программ для ИКТ, баз данных и аппаратных средств обеспечения сетевых технологий;

– отсутствие или несоответствие средств защиты информации современным информационным вызовам и угрозам;

– нарушение правил работы с охраняемой законом компьютерной информацией;

– низкий уровень специальной подготовки сотрудников правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере информационных технологий и безопасности;

– отсутствие скоординированной и комплексной государственной политики в сфере обеспечения информационной безопасности.

В настоящей работе мы остановимся на двух основных причинах киберпреступлений. Одна из них, как уже говорилось выше, это рост числа пользователей. В социологии имеется «правило 15 %», согласно ему, если население Земли вырастет на 15 %, то число совершаемых преступлений вырастет на 15 %. Данное правило также применимо и для киберпреступлений. Так, по данным «Лаборатории Касперского», в мире число хакерских DDoS-атак в 2019 г. выросло на 25 % по сравнению с 2017 г. и на 18 % – с 2018 г.[1]

По оценкам мировых экспертно-аналитических центров, каждую секунду 24 пользователя старше 18 лет становятся жертвами киберпреступности, таким образом, ежедневно от действий киберпреступников страдают более 2,4 млн человек. Количество жертв за 2021 г. составляет более 700 млн человек, каждый из которых в среднем теряет больше 421 долларов.

Особую актуальность вопросы противодействия преступлениям в сфере информационных технологий и безопасности приобретают в условиях мировой пандемии коронавируса. В этих условиях киберпреступники «переместили» свое внимание с простых людей и небольших организаций на государ-

[1] В «Лаборатории Касперского» отметили рост числа DDoS-атак в мире https://ria.ru/20190805/1557194818.html (дата обращения 20.01.2023).

ственные органы, учреждения здравоохранения и крупные корпорации, чтобы максимизировать свою прибыль и разрушения, вызванные коронавирусом. Из-за внезапного глобального перехода к удаленной рабочей среде во время пандемии коронавируса организациям пришлось быстро развертывать удаленные системы, сети и приложения. В результате возник риск уязвимости в обеспечении безопасности при организации удаленной работы.

Например, в 2020 г. поступило примерно 907 тыс. спам-сообщений, обнаружены 737 инцидентов, связанных с вредоносными программами, созданы 48 тыс. вредоносных URL-адресов, об этом говорится в докладе Интерпола.

Киберпреступники также пользуются растущим спросом на медицинские принадлежности, а также своевременной информацией о COVID-19, причем мошенники все чаще регистрируют доменные имена, содержащие соответствующие ключевые слова, такие как «coronavirus» или «COVID». Коронавирус можно назвать идеальной средой для совершения преступлений. Стресс и неопределенность, вызванные кризисом COVID-19, создают идеальную среду для киберпреступников, стремящихся обогатиться или создать хаос. Преступники не уклоняются от попыток воспользоваться этими возможностями, о чем свидетельствует их спешка с «обновлением» маршрута атак и использованием «фальшивых» новостей. Поскольку пандемия продолжается, «страх формирует неуверенность, а неуверенность и неопределенность приводят к плохой киберзащите», говорит адвокат Джейсон Вайс, эксперт по киберкриминалистике в юридической фирме Faegre Drinker, Biddle and Reath. По мере того, как пандемия коронавируса и карантинные меры затягиваются, и случаи заболевания продолжают расти, можно предположить, что масштабы киберпреступлений будут огромными, особенно по причине того, что экономика «слабеет» и люди будут страдать от финансовых последствий коронавируса. В связи с этим возникает необходимость ми-

нимизации и ограничения потенциальных угроз кибератак, а также улучшить систему кибербезопасности.

Как отмечается в докладе Управления ООН по наркотикам и преступности, посвященному вопросам киберпреступности и коронавируса COVID-19, «пандемия COVID-19 представляет собой беспрецедентный вызов для всего мирового сообщества. Многие перешли от традиционных способов совершения операций в режим онлайн, также поступили и преступники. В то время, как масштабы и изощренность киберпреступлений растет, и увеличивается количеств жертв, в некоторых странах представители правоохранительных органов вынуждены исполнять другие обязанности. Усугубляет ситуацию для общественности и правительств экономическое влияние COVID-19. Таким образом, складываются идеальные условия для потенциальных киберпреступлений».

Центральное место в современной кибепреступности занимает интернет-сеть Даркнет, которая изначально преследовала благие цели. Данная сеть состоит из интернет-сайтов, доступ к которым невозможен через общеизвестные поисковые системы («Google», «Yandex», «Rambler»). Информация внутри данных сайтов спрятана от большинства обычных пользователей обычной сети Интернет («Чистой сети»). Особенность ДаркНета состоит в том, что в ней практически невозможно отследить злоумышленника.

Дремлюга Р.И. отмечает, что использованию ДаркНета в преступных целях способствуют его следующие особенности[1]:

1. Анонимность, которая основана на так называемой «луковой» маршрутизации, обуславливающая невозможность отследить пользователя сети. Используя в качестве средства платежа криптовалюту, преступник делает невозможным отслеживание движения своих финансовых потоков.
2. Шифрование информации, передаваемой в Даркнете. Указанное обуслав-

[1] Дремлюга Р.И. Незаконный оборот наркотиков и крипторынки: угрозы и вызовы правоохранителю // Международное сотрудничество и зарубежный опыт. 2018. № 2. С. 33.

ливает трудности в противодействии нелегальной деятельности;

3. Трансграничная природа Даркнета, обусловленной стукнутой самой сети. Интернет позволяет совершать преступления на территории другого государства и способствует кооперации и консолидации международных преступных группировок и сообществ независимо от вида деятельности, но интернет-ресурсы (сайты) в сети Интернет, так или иначе, обладают географической или национальной привязкой. В отличие от сети Интернет имена сайтов Даркнета никак не отражают национальную принадлежность, а так как данные о сети хранятся распределено на территории многих стран. Для открытия сайта не требуется регистрация и следование национальным нормам.

Около 70% всех продавцов на крипторынках Даркнета предлагают наркотики, а не другие виды нелегального товара. Исследование, проведенное в январе 2016 г., показало, что на 8 крупнейших крипторынках (AlphaBay, Cryptomarket, Dark Net Heroes League, Dreammarket, French Dark Net, Hansa, Nucleus and Python) было размещено более 100 000 объявлений о продаже наркотиков и психоактивных веществ.

В связи с изложенным мы можем сделать вывод о том, что технология Даркнета была воспринята людьми как средство, которые может быть использовано в преступных целях, что не оправдало надежд, которые преследовались изначально создателями принципов его работы. А ведь на начальном этапе главными спонсорами разработок являлись ВМС США (2001-2006), Национальный научный фонд (2007), Google (2008-2009), Национальная исследовательская лаборатория США (2006-2010), Национальная христианская организация (2010-2012), Фонд Форда (2012-2014), Департамент США по защите прав (2013-2016), Министерство иностранных дел Германии (2015)[1].

В подавляющем большинстве случаев криптовалюта является основ-

[1] Безопасность электронного банкинга / А.М. Сычев, П.В. Ревенков, А.Б. Дудка. М., 2017. 293.

ным средством оплаты наркотиков. Первое серьезное упоминание криптовалюты в указанном качестве датируется 2013 годом в связи с расследованиями уголовного дела, связанного с Интернет-рынком «Silk Road» (Шелковый путь). Оплата за товары в подавляющем большинстве случаев производилась с использованием криптовалюты, а выбор в её пользу был сделан ввиду ее анонимности и трудностей технического характера установления и отслеживания финансовых транзакций[1]. Что примечательно, последующие проекты такие как «Evolution» и «Silk Road 2.0» посредством учета и устранения ошибок первого Интернет-рынка, смогли увеличить собственный доход на целых 100 млн. долларов США. При этом данные площадки обладали схожим функционалом, но лучшим дизайном, маркетингом и надежностью.

Если говорить о РФ, то на территории нашей страны в Даркнете действуют два крупнейших русскоязычных интернет-форума: «LegalRC» и «WayAWay». Цель данных форумов – реклама и продажа наркотических средств. Они содержат информацию о видах наркотиков, ценах, способах их приобретения, а также иных предметов и документов, запрещенных к в законном гражданском обороте. С конца октября 2016 г. также действует крупнейшая торговая площадка «HYDRA», в состав которой входит около 400 магазинов. Данный сайт имеет структуру, схожую с аналогичными ресурсами, действующими в ЕС и США. Сделки и оплата происходят непосредственно на площадке. Оплата производится исключительно с использованием криптовалюты Биткоин. Площадка охватывает все сферы теневого бизнеса, от продажи всех видов наркотиков до торговли поддельными документами, банковскими картами, оформленными на подставные данные, специального оборудования для слежки и съема информации, а также предоставления различных информационных услуг. Ресурсы сайта «HYDRA» размещаются на технических площадках хостинг- компании «Cloudflare» (США, Сан- Франциско).

Использование криптовалюты для покупки и продажи наркотиков на крипторынках означает, что операции в сети Даркнет становятся еще более анонимными. Именно поэтому все больше и больше преступников выбирают криптовалюты и крипторынки для своей нелегальной активности, сводя на нет попытки правоохранительных органов по пресечению их деятельности и обходя блокировки доступа к сетевым ресурсам.

В вопросе того, почему же криптовалюта является достаточно актуальным средством оплаты за незаконные товары и услуги, в том числе данных, которые могут быть использованы преступниками для совершения киберпреступлений в Даркнете, мы согласны с позицией С.И. Земцовой, П.В. Галушина,

А.Л. Карлов, которые в качестве черт, обуславливающих использование криптовалюты в преступных целях, выделяют следующие:

1 Децентрализация (нет централизованного сервера, который бы контролировал все операции. Этим одновременно «занимаются» взаимосвязанные сетью интернет-устройства;

2 Анонимность[1]. Данную характерную черту возможно трактовать как отсутствие явной связи между адресом, с которого происходит отправка криптовалют, и лицом, знающим секретный ключ и использующим его для совершения отправки. Однако следует сделать ремарку о том, что анонимность криптовалюты является все-таки достаточно условной, поскольку все адреса, записанное на них количество криптовалюты и все транзакции по приему и получению средств можно наблюдать в Интернете в реальном времени, и, как следствие, сам процесс использования криптовалют открыт и не является тайной. В связи с этим в некоторой литературе вместо «анонимности» предпочитают использовать такой термин как «псевдонимность», по-

[1] Родивиллин И.П., Родивиллина В.А. Криптовалюта как объект преступления // Деятельность правоохранительных органов в современных условиях: сборник материалов XXIII Международной научно-практической конференции. В 2-х томах. Иркутск. 2018. С. 262- 265.

скольку криптовалютный адрес выступает в определенном смысле псевдонимом обладателя[1].

3. Совершение транзакций в режиме P2P (равенство пользователей, транзакции осуществляются напрямую), нет посредников;

4. Невозможность налогообложения финансовых операций;

5. Высокая скорость обработки транзакций[2];

6. Мобильность криптовалюты как средства сбережения. Приватные ключи, представляющие собой сотни миллионов долларов, можно хранить на крошечном USB- накопителе и легко переносить в любое место»[3].

7. Трансграничность, которая обуславливает возможность криптовалюты перемещаться между любыми адресами ее блокчейна, что фактически означает мгновенность перемещений как между жителями одного города, так и между жителями разных государств[4].

8. Доступность, состоящая в возможности обращения к сервисам криптовалюты с помощью обычного мобильного телефона или иного устройства, подключенного к сети Интернет; отсутствие необходимости использования специальных банковских программно-аппаратных устройств.

Указанные признаки крипатовалюты позволяют ей функционировать вне банковского сектора, в связи с чем применение контроля со стороны банков и государственных органов невозможно.

Имеющиеся данные и прогнозы, сделанные ООН, позволяют нам сделать вывод, что криптовалюта оказала достаточно серьезное влияния на раз-

---

[1] Berentsen A., A Short Introduction to the World of Cryptocurrencies // Federal Reserve Bank of St. Louis Review. First Quarter 2018. 100 (1). P. 1 - 16. [Электронный ресурс] URL: https://files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf (дата обращения: 01.02.2023г.).

[2] Кучеров И.И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. 2018. № 2. С. 17-21.

[3] Долгиева М.М. Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. 2019. № 4. С. 128-139.

[4] What is Ripple? [Электронный ресурс] URL:https://www.alphr.com/cryptocurrency/1009741/what-is-ripple (дата обращения: 21.01.2023).

витие наркопреступности, расширив сферу влияния последней, её возможности, каналы поставок и сбыта. Приобретение наркотиков стало более анонимным, и, как следствие, безопасным как для потребителей, так и для организаторов.

Человеческое общество так устроено, что на каждое действие (технологию, явление и т.д.), создается противодействие, нивелирующее плюсы и достоинства первого. Указанное философское положение справедливо и для криптовалюты. В данном случае мы говорим о разработке программ по идентификации пользователей криптовалютных сервисов.

Одним из таких сервисов является «Crystal» от поставщика блокчейн-решений «Bitfury Group». Цель данного сервиса состоит в выявлении и расследовании криминальной деятельности в блокчейне «Биткойн» путем отслеживания перемещения подозрительных транзакций до конечного получателя или точки сбыта криптовалюты правоохранительными органами. Структура блокчейна Биткойна содержит информацию обо всех транзакциях, доступную всем участникам сети. Алгоритмы сервиса «Crystal» загружают и обновляют данные из блокчейна, а также собирают в сети Интернет публично доступную информацию о владельцах кошельков криптовалюты. При этом вся информация обрабатывается так, что данные в дальнейшем были пригодны для аналитики и могли быть представлены пользователю в удобном формате. Результаты обработки сохраняются в заде данных.

Основными критериями назначения степени риска являются подтвержденная публичная информация о нелегальной деятельности конкретных участников блокчейна Биткоина и наличие транзакций с ними прочих участников. Например, если участник А. взаимодействовал с известным высокорисковым участником В., то участник А. также «попадает под подозрение», то есть алгоритм присваивает ему некий повышенный уровень риска. Наличие или отсутствие риска отображается в интерфейсе приложения с помощью красных и зеленых меток соответственно. При этом «Crystal» является

аналитическим инструментом и не дает оценок законности транзакций. Считать ту или иную транзакцию сомнительной или незаконной прерогатива правоохранительных органов.

Отслеживать информацию о транзакциях может либо сам пользователь «Crystal», либо сторонняя программа: «Crystal» содержит API для интеграции с аналитическим программным обеспечением пользователя. Сбор персональных данных «Crystal» не производит.

Разработчики отмечают, что лежащие в основе анализа данных эвристические алгоритмы, по своей природе не дают стопроцентного результата. Поэтому решения, выносимые сервисом «Crystal», не являются категоричными – все остается в зоне ответственности пользователя. Интерес к данному инструменту с момента создания был проявлен со стороны финансового сектора (банков, консалтинговых компаний, финансовых регуляторов), а также киберподразделений силовых структур.

Наряду с ним, в конце 2018 года был представлен «Know Your Transaction» (KYT) компанией «Chainalysis». Цель данного сервиса состоит в отслеживании людей, которые участвуют в незаконной деятельности, связанной с криптовалютами. Среди постоянных клиентов «Chainalysis» – Федеральное бюро расследований США (ФБР), Администрация по борьбе с наркотиками (DEA) и Европол. Продукт «KYT» от «Chainalysis» предоставляет обратную связь по транзакциям в реальном времени и отправляет соответствующую информацию на биржу в «движок обработки транзакций».

Существует точка зрения, согласно которой криптовалюта выступает характерным примером инновации экономики террора. Именно использование криптовалют позволяет террористам посредством задействования новых финансовых механизмов обеспечивать независимость экономики террора от легальных экономических структур в процессе производства и потребления необходимых им товаров и услуг. Создаваемые террористами собственные каналы перемещения финансовых средств на основе использования современ-

ных альтернативных платежных систем позволяют доставлять необходимое финансирование преступным группам по всему миру. При этом констатируется, что инновационный характер криптовалюты делает практически бессмысленными все ранее существовавшие меры борьбы международных организаций и государств с финансированием террористических организаций и групп[1].

По данным руководителя рабочей группы Госдумы Российской Федерации по оценкам рисков оборота криптовалюты, доктора юридических наук Э.Л. Сидоренко, в 2015 году количество зафиксированных фактов использования виртуальной валюты для отмывания преступных доходов не превышало 5 % от общего объема криптовалюты, а в 2018 г. этот показатель превысил 40%[2].

В 2018 году в сфере противодействия легализации (отмыванию) доходов от незаконного оборота наркотиков в отчетном периоде зарегистрировано 309 преступлений по фактам легализации (отмывания) доходов, полученных от незаконного оборота наркотиков, что в 1,9 раза (на 86,1%) превышает показатель прошлого года (166). Установленная сумма легализованных наркодоходов (денежных средств или иного имущества по оконченным предварительным расследованием уголовным делам) в 1,7 раза (на 67%) превысила показатель прошлого года, составив 381 млн. 525 тыс. рублей (2017 – 228 млн. 398 тыс. руб.). Значительных результатов удалось достичь благодаря организации эффективного взаимодействия с компетентными органами и подразделениями финансовой разведки государств СНГ и иных зарубежных стран.

Справедливости ради следует оговориться, что использование криптовалюты в преступных целях хотя и имеет место, тем не менее не может быть

[1] Сальников Е.В. Сальникова И.Н. Криптовалюта как иновация экономики терроpора // Науковедение. 2016. № 3. С. 33.

[2] Сидоренко Э.Л. Наркотики и криптовалюта: новые криминологические тренды // Наркоконтроль. 2018. № 2. С. 8-13.

однозначно охарактеризовано как тотальное. К примеру, Управлением по борьбе с наркотиками США (DEA) констатировано сокращение доли использования Биткойна в преступной деятельности. Как отметили представители этого правоохранительного ведомства, большинство переводов носят преимущественно спекулятивный характер и лишь примерно каждая десятая транзакция имеет криминальную подоплеку, хотя в номинальном выражении объем последних за последние пять лет значительно возрос. Одновременно обращено внимание на то, что отсутствие традиционных финансовых посредников и администраторов в криптовалютных платежных системах создает известные проблемы при расследовании, которые, впрочем, являются устранимыми[1].

В общем виде схема легализации преступных доходов выглядит следующим образом:

1. Конвертирование наркоденег в криптовалюту;
2. Перевод криптовалюты в любую валюту по выбору;
3. Обналичивание денежных средств.

Как отмечает В.А. Ализаде и А.Г. Волеводза, «организаторы и руководители преступных организаций, деятельность которых сосредоточена в сфере незаконного оборота наркотиков, распределяют денежные средства, полученные от преступной деятельности, между их участниками, предварительно совершая с ними операции по переводу денежных средств в криптовалюту, и в таком виде по каналам сети Интернет направляют конкретным исполнителям на счета их электронных кошельков (чаще всего «QIWI-кошельки»). Получатели криптовалюты в последующем на онлайн-биржах обменивают их на рубли и используют в своих целях. Деньги с использованием программ Интернет-банкинга переводятся с дроблением сумм платежей, а именно —

[1] Russo, Camila. Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now. Bloomberg. [Электронный ресурс] URL: https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now?srnd=cryptocurriences (дата обращения: 12.01.2023 г.).

путем проведения финансовых операций через системы денежных переводов без открытия счета в суммах менее 15 000 руб. Это позволяет избежать идентификации участников финансовых операций и обеспечить уклонение от процедур обязательного контроля со стороны кредитной организации[1].

Центральное место в легализации преступных доходов с использованием криптовалюты занимают криптобиржи (криптосервисы) различных типов. К указанным можно отнести следующие варианты:

1) Одноранговых транзакции типа «человек-человек»;

2) «Биткойн»-автоматов (криптоматов, криптотерминалов);

3) Смесителей, позволяющих запутывать цепочки транзакций. Например, некоторые из них устроены так, что один пользователь может купить за криптовалюту товар, необходимый для другого пользователя, а последний, в свою очередь, отправляет преступнику реальные деньги за вычетом определенной суммы (аналогия банковской комиссии). В данном случае выигрывают оба – преступник получает реальные деньги, а покупатель – товар со скидкой;

4) Нелегальных обменных сервисов. К указанным можно отнести 365cash.com, NetEx24.com, Z-exchange.com, 100btc.pro, Buy-Bitcoins.com и другие. Данные сервисы предоставляют возможно обмена криптовалют на рубли;

Онлайн-игр. Согласно аналитическому отчету компании «Trend Micro», преступники все чаще стали использовать одновременно виртуальную и игровую валюту ввиду отсутствия их правового статуса для легализации преступных доходов. Для этого покупается валюта игр Minecraft, FIFA, World of Warcraft, Final Fantasy, Star Wars Online, GTA 5, NBA и Diablo. В последующем она продается за криптовалюту, а криптовалюта обменивается на специальных сервисах конвертации.

[1] Ализаде В.А. Волеводз А.Г. Судебная практика применения ст. 174¹ УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты // Наркоконтроль. 2017. № 4. С. 9.

Таким образом подводя итоги рассмотрению вопроса следует подчеркнуть, что детерминанты киберпрестулений довольно разнообразны. Они связанны как с самими процессами, происходящими в обществе в последние годы, в частности: увеличение объема данных создаваемых, хранящихся и передаваемых по средством информационно-коммуникационных технологий; тенденция к переходу к оплате от наличных денежных средств к безналичным; появление новых средств платежей, а в частности криптовалюты. Также детерминанты киберпреступности напрямую связаны с слабой работой правоохранительных органов в данной сфере, малочисленностью специализированных кадров по выявлению и пресечению данного вида преступлений, виктимным поведением самих потерпевших, которые предоставляют злоумышленникам свои данные, которые позволяют совершить киберпреступление, отсутствием хорошего программного обеспечения по защите данных пользователей, в том числе государственных учреждений, что приводит к возможности совершения киберпреступлений.

1.3. Личность лица, совершающего киберпреступления

При анализе детерминантов киберпреступлений существенное значение имеет анализ личности преступника в сфере информационных технологий и безопасности.

Анализируя личность киберпреступника прежде всего необходимо обратить внимание на их классификацию и типологию, являющимися видами систематизации лиц, совершающих киберпреступления.

Под классификацией преступников понимается наиболее простой уровень обобщения преступников по одному группировочному признаку, например по полу, возрасту, месту жительства, роду занятий, наличию судимостей и т.д. Классификация осуществляется с целью выявления наиболее общих и распространенных особенностей и тенденций, на основании эмпирических данных. Классификация лиц, совершивших киберпреступления, позволяет обратить внимание на криминологический портрет киберпреступника.

Черты преступников в сфере информационных технологий и безопасности позволяют нам выделять следующие типы:

1. «Новичок». Данная категория личности совершает правонарушения впервые и характеризуется использованием различных информационных технологий (персональный компьютер, ноутбук) для личных потребительских целей: для загрузки музыки, игр или приложений. В основном это – подростки или молодежь в возрасте 15-25 лет. Пол – в подавляющем большинстве случаев мужской. Образование – среднее, среднее специальное или высшее.

2. «Любитель». Данная категория личности представляет собой лиц, которые периодически совершают правонарушения в компьютерной сети, в основном – это технический персонал (системные администраторы, технические консультанты). В данную группу входят лица мужского пола (реже женского) в возрасте от 20-30 лет. Формирование «любителей» происходит от навыков прошлого в качестве «новичка» или в связи с жизненными обстоятельствами (выполнение поручений и «заказов»).

3. «Профессионал». Данная категория профессиональных лиц, на профессиональной основе занимающихся неправомерной деятельностью и име-

нуемых хакерами. Это – класс образованных лиц, знающих все азы компьютерного программирования и технической работы. Возраст – 25- 40 лет. Пол – в большинстве случаев мужской. Д. Букин справедливо отмечает, что высокая техническая подготовленность – их основная черта, высокая латентность преступлений – основа их мотивации, внутренняя предрасположенность – основное условие вступления на преступный путь и социально-экономическая ситуация в стране – основная причина окончательного выбора[1].

В рамках рассматриваемого вопроса представляют особый интерес виды компьютерных преступников.

По целям и сфере преступной деятельности всех компьютерных преступников можно разделить на отдельные подгруппы[2]:

1. Хакеры (hacker) – пользователи вычислительных систем и сетей ЭВМ, которые занимаются поиском незаконных методов получения несанкционированного (самовольного) доступа к средствам компьютерной техники и баз данных, а также их несанкционированным использованием с корыстной целью. По общему мнению, хакеры – это компьютерные хулиганы, которые без разрешения проникают в чужие информационные системы ради забавы. В значительной степени их, в первую очередь, привлекает преодоление трудностей. В настоящее время правоохранительные органы обеспокоены появлением так называемых «белых хакеров».

Это новые социальные образования, ставящие целью на более высоком уровне овладеть методами несанкционированного доступа к информационным системам. Лидеры таких образований объясняют, что они не используют свои знания для нападения, а исследуют слабые места операционных систем для их усовершенствования.

---

[1] Кардава Н.В. Киберпространство как новая политическая реальность: вызовы и ответы // История и современность. 2018. №1-2. С. 27-28.

[2] Сорокин, А.В. Компьютерные преступления: уголовно - правовая характеристика, методика и практика раскрытия и расследования // Электронный ресурс. - http://kurgan.unets.ru/~procur/my_page.htm

2. Кракеры (cracker) – разновидность хакеров. Это более серьезные нарушители, способные причинить какой-либо вред системе. Кракер, осуществляя взламывание компьютерной системы, действует с целью получения несанкционированного доступа к чужой информации. Мотивы этого доступа могут быть различными: хулиганские побуждения, озорство, месть, корыстные мотивы, промышленный и иной шпионаж и т.д.

Выделяют три группы «кракеров»:

а) «вандалы» - наиболее известная группа преступников (во многом благодаря огромной распространенности вредоносных программ, авторами которых они чаще всего выступают). Их основная цель заключается во взломе компьютерной системы для ее последующего разрушения (уничтожение файлов, форматирование жесткого диска компьютера, влекущее потерю хранящейся на нем информации, и пр.);

б) «шутники» - наиболее безобидная (с точки зрения ущерба для компьютерной информации) часть «кракеров». Их основная цель – взлом компьютерной системы и внесение в нее различных звуковых, шумовых, визуальных эффектов. Мотив - игровой;

в) «взломщики» - профессиональные преступники, осуществляющие взлом компьютерной системы с целью хищений денежных средств, промышленного и коммерческого шпионажа, хищений дорогостоящего программного обеспечения и т.д. Совершаемые ими преступления носят серийный характер. «Взломщики» могут действовать как в своих собственных интересах, так и в интересах других лиц.

3. Фрикер (phone + break = phreak) – специализируются на использовании телефонных систем с целью избежания оплаты телекоммуникационных услуг. Их преступная деятельность направлена на получение кодов доступа, хищение телефонных карточек и номеров доступа с целью перенести оплату на телефонные разговоры на счет другого абонента.

4**.** Кардеры – оплачивают свои расходы с чужих кредитных карточек.

5. Коллекционеры (codes kids) – коллекционируют и используют программы, перехватывающие различные пароли, а также коды телефонного вызова и номера частных телефонных компаний, которые имеют выход в общую сеть.

6. Кибервороны – злоумышленники, которые специализируются на несанкционированном проникновении в компьютерные системы финансовых, банковских расчетов. Используют компьютерные технологии для получения номеров кредитных карточек и другой ценной информации с целью наживы. Нередко полученную информацию они продают другим лицам.

7. Компьютерные пираты – специализируются на незаконном взломе систем защиты лицензионных компьютерных программных продуктов, которые потом распространяются за деньги. Торгуют ими по ценам, которые значительно ниже цен законных изготовителей.

Исходя из вышеперечисленных групп, можно утверждать, что киберпреступник характеризуется технической подготовленностью, обладает набором методов, позволяющих ему осуществлять различные махинации (получение несанкционированного доступа, взлом ключей безопасности и т. д.). В большинстве случаев это выпускник (или студент старших курсов) технического вуза, имеющий свой персональный компьютер или ноутбук. В подавляющем большинстве случаев – это мужчины в возрасте 15-40 лет. Как правило, изучаемые лица имеют замкнутый характер, зачастую депрессивны, склонны к личностным переживаниям, обидчивы. Их успехи в школе не были блестящи, но основы информатики и математику они учат хорошо. В большинстве своем они, возможно, имеют неполную семью, где царит сложная психологическая атмосфера. Согласно статистическим данным, 72,2 % хакеров жили в момент совершения преступления с одним из родителей, в 51,3 % случаев основной успех хакеров в обучении был в точных науках,

33,1 % начинали свою деятельность с желания испробовать технику компьютерного взлома[1].

Для киберпреступников характерны правовой нигилизм и завышенная самооценка, в большинстве случаев они, чувствуя свою безнаказанность и неуязвимость, пренебрегают требованиями норм закона и считают вполне нормальным самостоятельно определять моральность и правильность тех или иных правовых норм, исходя из собственных критериев. Часто проявляют инфантилизм, безответственность, бескомпромиссность, непонимание возможных последствий своих действий, нередко игнорируют общественное мнение и интересы. В подобных случаях «оценка ситуации осуществляется не с позиций социальных требований, а исходя из личных переживаний, обид, проблем и желаний»[2]. В качестве мотивов преступления – различных побуждающих факторов, которые способствуют совершению киберпреступлений – можно отнести корысть (большинство киберпреступлений совершается из корыстных побуждений), политические и религиозные взгляды, хулиганство.

Типология киберпреступников – наиболее высокий уровень систематизации, в основе которой лежат наиболее существенные признаки, позволяющие обратить внимание на мотивационную сферу, психологические (индивидуальные) детерминанты преступности, а также уровень вовлеченности в преступную деятельность.

В связи с чем следует выделить следующие типы киберпреступников:

– начинающий тип киберпреступника (средний материальный достаток, возможность владеть компьютерными устройствами (одним или более); возраст – от восемнадцати до тридцати лет; преимущественно лица мужского пола с техническим образованием (среднее, среднее специальное или высшее

[1] Очилов Х.Р. Некоторые суждения о проблемах квалификации хищения чужого имущества с использованием компьютерных средств в условиях нынешних судебно-правовых реформ. // Review of law sciences. 2020. № 4. С. 205-210.

[2] Антонян Ю.М., Еникеев М.И., Эминов В.Е. Психология преступника и расследования преступлений. М., 2006. С. 120.

(в ряде случаев – неоконченное)); деятельность – либо профессиональная деятельность, коррелирующая с информационными и компьютерными технологиями (специалисты компьютерных фирм, администраторы баз данных и т.д.), либо отсутствие постоянной работы);

– устойчивый киберпреступник (средний и выше среднего материальный достаток, наличие глубоких познаний в сфере информационных технологий, сетей, иных достижений цифрового общества; возраст – средний, от двадцати до двадцати пяти лет; преимущественно мужской пол с тенденцией проявления активности лиц женского пола (5%); образование – преимущественно – высшее техническое или аналогичное неоконченное высшее; наличие возможности владеть инновационными компьютерными системами, устройствами, компьютерными разработками);

– профессиональный киберпреступник (высокий уровень материальной обеспеченности; возраст – выше двадцати пяти лет; преимущественно лица мужского пола (доля лиц женского пола – 8%); образование – высшее техническое, наличие профессиональных познаний, навыков, умений в сфере информационных технологий, сетей, иных достижений цифрового общества на высоком уровне, постоянное совершенствование навыков в сфере применения средств для совершения киберпреступлений, в т.ч. разработанных лично)[1].

Обобщая данные авторов, занимающихся активной разработкой данной проблематики, можно обобщить, что личность киберпреступника довольно нетрадиционна и имеет свои особенности. Первая особенность, по нашему мнению, заключается в низком возрасте, так лица склонные совершать киберпреступления как правило являются активными пользователями и отлично разбираются в различных аспектах, связанных с компьютерной техникой с самого детства. Следующей особенностью данных лиц является их скрыт-

[1] Гаврило Ю.В., Аносов А.В., Баранов В.В. Деятельность ОВД по борьбе с преступлениями, совершѐнными с использованием информационных, коммуникационных и высоких технологий: Учебное пособие. М., 2019. Ч. 1. С. 52.

ность, так как зачастую киберпреступники незаметны в обычной жизни и большую часть своего свободного времени проводят сидя за компьютером как правило дома, при этом обладая знаниями по скрытию следов в информационной сети они успешно меняют адреса доменов существенно усложняя задачу по своей поимке.

ГЛАВА 2. ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

2.1. Понятие, объекты и субъекты профилактики киберпреступности

Под криминологическим предупреждением киберпреступности понимается деятельность государства, общества и отдельных лиц, осуществляемая через меры принуждения, воспитания, оказания помощи лицам, подвергающимся профилактическому воздействию, с целью устранения детерминантов киберпреступлений.

Элементами криминологического предупреждения выступают: объекты предупреждения, меры предупреждения, субъекты предупреждения. Объекты предупреждения включают негативные явления и процессы, лиц и группы, которые воспроизводят преступность. Меры предупреждения преступности характеризуют механизм профилактического воздействия. Субъекты предупреждения дают представление о носителях активности этой деятельности[1].

Традиционно выделяются два вида криминологического предупреждения преступности:

– общекриминологическое предупреждение;

– специально-криминологическое предупреждение.

По нашему мнению, полностью преступность никогда не перестанет существовать, однако следует принять, что каждое из них наносит неизгладимый вред отдельно взятому человеку, группе лиц и в целом общественным отношениям. Одной из главных задач государства в лице своих органов является борьба с преступностью и причинами ее порождающими. В криминологии предупреждением преступности принято считать многоуровневую сис-

[1] Шеслер А.В. Групповая преступность: криминологические и уголовно-правовые аспекты: дис. д-ра юрид. наук. Екатеринбург, 2000. С. 188.

тему государственных и общественных мер, направленных на выявление, устранение, ослабление или нейтрализацию причин и условий преступности, ее отдельных видов и конкретных деяний, а также на удержание от перехода или возврата на преступный путь людей, условия жизни и (или) поведение которых указывает на такую возможность[1].

Изучая понятие «предупреждение преступности» или «профилактику преступлений», в том числе наркопреступлений совершаемых мигрантами, необходимо уяснить сущность таких понятий, как «объект», «предмет» и «субъект» предупреждения.

Объект предупреждения – это общественные отношения, связанные с нарушением действующего законодательства, норм морали и других правил поведения в обществе. Предмет предупреждения – это конкретное поведение лица (группы лиц)[2].

Общим объектом предупреждения преступности являются условия и причины преступлений и преступности, а именно криминогенные социальные явления, обуславливающие виды, состояние и динамику преступности, а также негативные воздействия на микроуровне.

Применительно к объекту предупреждения рассматриваемой категории преступлений объектом предупреждения являются общественные отношения связанные с институтами собственности, коммерческих, врачебных и частных и иных видов тайн, интеллектуальной собственности, чести и достоинства граждан, которые нарушаются в следствии кибератак.

Кроме того, объектом предупреждения киберпреступлений, является незаконное поведение лиц, связанное с совершением кибепреступлений.

Под субъектами предупреждения преступности в криминологической литературе понимают «государственные органы и общественные организа-

---

[1] Криминология: учебник для студентов вузов / под ред. Н.Ф Кузнецовой, В.В. Лунеева. М., 2005. С. 185.

[2] Архипцев И.Н. Некоторые аспекты противодействия и профилактики преступлений, совершаемых иностранными гражданами и лицами без гражданства в России // Научные ведомости. 2012. № 14. С. 45.

ции, а также должностных лиц и граждан, целенаправленно осуществляющих, на различных уровнях и в различных масштабах, меры, направленные на выявление и устранение причин преступности и условий, способствующих совершению преступлений»[1]. Таким образом в своем единстве указанные субъекты представляют систему, которая на различных уровнях борется и превращает негативные проявления, которые влияют на детерминанты преступности, в том числе киберпреступлений.

Обычно субъекты предупреждения преступности делят на три группы[2]:

1) субъекты общесоциального предупреждения – федеральные, региональные и местные органы власти и управления, общественные организации, не выполняющие непосредственные правоохранительные задачи;

2) субъекты специального предупреждения: а) государственные правоохранительные органы, непосредственно выполняющие правоохранительные функции (например, МВД, ФСБ, ФСИН и т.д.); б) государственно-общественные структуры, не являющиеся правоохранительными органами, но выполняющие правоохранительные функции (например, комиссии по делам несовершеннолетних); в) частные и общественные структуры, содействующие выполнению правоохранительных задач (например, частные охранные предприятия);

3) субъекты индивидуального предупреждения, т.е. конкретные люди, взаимодействующие с потенциальными правонарушителями, – соседи; родители и лица, их заменяющие; супруги; отдельные граждане, «вынужденные» общаться с такими людьми в силу сложившихся обстоятельств (учителя, преподаватели, сослуживцы по работе и т.д.). То есть предупреждением преступности, помимо правоохранительных органов, занимается широкий круг

[1] Долгова А.И. Понятия советской криминологии / А.И. Долгова, Б.В. Коробейников, В.Н. Кудрявцев, В.В. Панкратов. М., 1985. С. 83.

[2] Горшенков Г.Н. Криминология и профилактика преступлений / Г.Н. Горшенков, Е.А. Костыря, О.В. Лукичев и др. СПб., 2001. С. 101; Криминология: Учебник для вузов / Под ред. В.Н. Бурлакова, Н.М. Кропачева. СПб., 2003. С. 184 - 185.

организаций, учреждений и простых граждан, деятельность которых нужно учитывать при рассмотрении данного вопроса.

По вертикали структуру предупредительной деятельности можно разделить на три уровня: 1) федеральный уровень, который предусматривает следующие мероприятия: а) координацию всей предупредительной деятельности; б) выявление региональных ресурсов; в) научно-методическое и нормативно-правовое обеспечение; г) определение минимального стандарта предупредительных, профилактических и реабилитационных мероприятий; д) контроль за ходом реализации региональных программ по предупреждению преступности, особенно – по ее профилактике. При этом на государственном уровне должна быть решена одна из важнейших задач предупреждения преступности – удовлетворение основных жизненных потребностей человека, детерминирующих его здоровый образ жизни (нормальные жилищные условия и полноценное питание, доступность медицинской помощи семьям, специализированная социально-психологическая поддержка и др.);

2) региональный уровень (субъекты Федерации), который: а) привлекает местные ресурсы; б) разрабатывает стратегию реализации региональной программы по предупреждению преступлений, с опорой на кадровый потенциал специалистов, осуществляющих предупредительную деятельность; в) практически реализует профилактические и иные программы по предупреждению преступности; г) учитывает специфику региональных условий (социально-экономических, этнокультурных, демографических, климатогеографических и др.); д) учитывает предшествующий позитивный и негативный опыт работы по предупреждению преступлений; е) контролирует ход реализации региональной программы;

3) местный уровень, который непосредственно осуществляет основную часть специально-криминологической и индивидуальной профилактической и иной предупредительной деятельности.

Применительно к субъектам борьбы с кибепреступлений указанная вертикаль имеет место быть, и все ее звенья выполняют отведенную ей функцию. Конечно, основными субъектами предупреждения кибепреступлений являются правоохранительные органы, которые в пределах своей компетенции осуществляют борьбу по различным направлениям.

Справедливо утверждение П.Н. Кобеца, отметившего, что предупреждение преступлений – это сложный, многогранный процесс, обладающий определенными признаками целостности, который целесообразно рассматривать комплексно, выделяя его составляющие элементы[1].

По мнению В.Е. Эминова и И.М. Мацкевича, предупреждение преступности – это многоуровневая система мер и осуществляющих их субъектов, направленная на: а) выявление и устранение либо ослабление и нейтрализацию причин преступности, отдельных ее видов, а также способствующих им условий; б) выявление и устранение ситуаций на определенных территориях или в определенной среде, непосредственно мотивирующих или провоцирующих совершение преступлений; в) выявление в структуре населения групп повышенного криминального риска и снижение этого риска; г) выявление лиц, поведение которых указывает на реальную возможность совершения преступлений, и оказание на них сдерживающего и корректирующего воздействия, а в случае необходимости – и на их ближайшее окружение[2].

Считаем, что определение о том, что следует понимать под предупреждением преступности, сформулированное признанным классиком российской криминологии В.В. Лунеевым, наиболее полно вобрало в себя все изложенные нами позиции авторов по этому вопросу.

Под предупреждением преступности В.В. Лунеев понимает совокупность различных взаимосвязанных между собой мер, проводимых правоох-

---

[1] Кобец П.Н. Современное состояние теории предупреждения преступности и ее роль в оптимизации борьбы с преступлениями // Российская юстиция. 2012. № 1. С. 19.

[2] Криминология: Учебник / Под ред. В.Н. Кудрявцева и В.Е. Эминова. М., 2007. С. 265 - 266.

ранительными и иными государственными органами и общественными организациями, а также отдельными гражданами и направленных на предотвращение уголовно наказуемых деяний в семье, школе, общественных местах, на производстве, в городе, области, стране и минимизацию причин, порождающих преступность[1]. Таким образом мы видим, что автор показывает взаимосвязь всех элементов предупреждения преступлений, таких как объект, предмет и субъекты, что в своей совокупности позволяет наиболее полно подходить к выстраиванию предупредительной работы, в том числе и применительно к вопросам предупреждения наркопреступности.

Подводя итоги рассмотрению вопроса отметим, что предупреждение характеризуется наличием четких элементов, таких как объект, предмет и субъекты, что в своей совокупности позволяет наиболее полно подходить к выстраиванию предупредительной работы, в том числе и применительно к вопросам предупреждения наркопреступности. Применительно к объекту предупреждения рассматриваемой категории преступлений объектом предупреждения являются общественные отношения связанные с институтами собственности, коммерческих, врачебных и частных и иных видов тайн, интеллектуальной собственности, чести и достоинства граждан, которые нарушаются в следствии кибератак. Предметом же киберпреступлений, является незаконное поведение лиц, связанное с совершением кибепреступлений. Субъекты предупреждения киберпреступлений могут быть условно разделены на ряд групп, в зависимости от классификационного признака. В частности, в своем вертикале субъекты могут быть представлены на федеральном, региональной и местном уровнях. Применительно к субъектам борьбы с киберпреступлений указанная вертикаль имеет место быть, и все ее звенья выполняют отведенную ей функцию. Конечно основными субъектами предупреждения киберпреступлений мигрантов являются правоохранительные органы, которые в пределах своей компетенции осуществляют борьбу по раз-

[1] Лунеев В.В. Курс мировой и российской криминологии: учебник. В 2 т. Т. I. Общая часть. М., 2011. С. 925-926.

личным направлениям. Также существует классификация в зависимости от уровней предупреждения, а именно субъекты общего, специального и индивидуального предупреждения. В данной классификационной группе главную роль выполняют органы специального предупреждения.

2.2. Общекриминологическая профилактика киберпреступности

Содержание мер общекриминологического предупреждения киберпреступности состоит в реализации общегосударственных социально ориентированных программ, укрепляющих антикриминогенный потенциал общества. Субъектами реализации данных мер являются государственные органы Российской Федерации и субъектов Российской Федерации, муниципальные образования, реализующие социальные программы, создаваемые при их содействии общественные организации, деятельность которых связана с реализацией общесоциальных программ в обществе.

Проведенный анализ специальной и научной литературы показывает, что вопросам уголовно-правовой защиты компьютерной информации и противодействия компьютерным преступлениям в Российской Федерации уделяется пристальное внимание как со стороны государства, так и со стороны научного сообщества[1].

По мнению авторов, целью предупреждения компьютерной преступности выступает обеспечение в Российской Федерации необходимых условий для безопасного создания, обработки и распространения компьютерной информации, а также нормального функционирования компьютерных устройств и информационно-телекоммуникационных сетей.

[1] Родивилин И.П. Проблемы квалификации преступлений в сфере компьютерной информации, совершаемых с использованием дистанционного управления банковским счетом, и их предупреждение // Пролог. 2014. № 2 (6). С. 61–64.

В свою очередь, мы полагаем, что к основным задачам превенции данного вида преступности относится выработка и реализация комплекса мер, направленных на предотвращение:

– преступных посягательств на основы конституционного строя, общественную безопасность и общественный порядок в РФ;

– угроз информационной безопасности личности, общества, государства, т.е. обеспечение возможности безопасного создания, хранения, обработки и передачи вышеуказанными субъектами права не запрещенной законом компьютерной информации;

– несанкционированных действий, направленных на уничтожение, блокирование, модификацию, копирование компьютерной информации или нейтрализацию средств защиты компьютерной информации физических и юридических лиц, либо угрозы причинения указанных последствий;

– противоправных действий, направленных на нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям;

– угроз информационной безопасности коммерческих и некоммерческих организаций, государственных (муниципальных) органов власти, предприятий и учреждений, связанных с обеспечением режима тайны конфиденциальной информации (персональных данных и информации частного характера, сведений, представляющих государственную, служебную, профессиональную, коммерческую и иную тайну);

– несанкционированных действий, направленных на нарушение работы средств защиты, хранения, обработки и передачи компьютерной информации на военных, стратегических и социально значимых объектах (транспортных, промышленных, энергетических, научных, здравоохранительных, образовательных и т.д.);

– нарушения конституционных прав граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом, неприкосновенность частной жизни, личной и семейной тайны, собственности и др.[1]

Содержание указанных задач, по нашему мнению, позволит определить круг мер общего и специального характера, направленных на предупреждение компьютерных преступлений.

Анализ научной литературы позволяет выделить следующие подходы к освещению данной проблематики. С позиции Т.М. Лопатиной, система мер предупреждения компьютерных преступлений должна быть комплексной и включать в себя, с одной стороны, организационно-управленческие, технические (физические) меры, с другой — кадровые (в сочетании с морально-этическими) и правовые[2].

Не подвергая сомнению приведенные позиции, можно согласиться с точкой зрения Т.М. Лопатиной, согласно которой система профилактических мер, направленных на предупреждение компьютерных преступлений, должна носить комплексный и многосторонний характер. Между тем, учитывая методологический подход криминологической науки, мы выделяем меры общей превенции (например, политические, экономические, социальные, научно-технические, духовно-культурные) и специальные превентивные меры (правовые, духовно-культурные, организационно-управленческие, технические, криминалистические и др.).

Общепревентивные меры предупреждения компьютерных преступлений носят всеобщий характер и направлены на профилактику как компьютерной преступности в частности, так и преступности в целом.

---

[1] . Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации // Академический юридический журнал. 2015. № 1 (59). С. 25–26.

[2] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дисс. ... д-ра юрид. наук. М., 2007. С. 316.

Достаточно ясно и лаконично, на наш взгляд, они сформулированы в Указе Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 02 июля 2021 г. № 400.

Например, к общеполитическим мерам предупреждения преступлений в сфере компьютерной информации в России можно отнести: развитие демократии и гражданского общества, обеспечение незыблемости конституционного строя, территориальной целостности и суверенитета Российской Федерации; превращение Российской Федерации в мировую державу, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях многополярного мира.

Общеэкономические превентивные меры включают: повышение конкурентоспособности национальной экономики; экономический рост, который достигается прежде всего путем развития национальной инновационной системы и увеличения инвестиций в человеческий капитал; повышение производительности труда и др.

Общие социальные меры предполагают: снижение уровня социального и имущественного неравенства населения, стабилизацию его численности в среднесрочной перспективе, а в долгосрочной перспективе — коренное улучшение демографической ситуации; обеспечение личной безопасности, а также доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты активной трудовой деятельности и т.д.

К научно-техническим общепревентивным мерам относятся: формирование системы целевых фундаментальных и прикладных исследований и ее государственной поддержки в интересах организационно-научного обеспечения достижения стратегических национальных приоритетов; создание сети федеральных университетов, национальных исследовательских университетов, обеспечивающих в рамках кооперационных связей подготовку специалистов для работы в сфере науки и образования, разработки конкурентоспо-

собных технологий и образцов наукоемкой продукции, организации наукоемкого производства и др.

Духовно-культурные меры общей превенции включают: признание первостепенной роли культуры для возрождения и сохранения культурно-нравственных ценностей, укрепления духовного единства многонационального народа Российской Федерации и международного имиджа России в качестве страны с богатейшей традиционной и динамично развивающейся современной культурой, создание системы духовного и патриотического воспитания граждан России.

2.3. Специально-криминологическая профилактика Киберпреступности

Объектом специально-криминологического предупреждения киберпреступности являются лица, совершившие преступления, а также лица с социально отклоняющимся поведением. Основными специализированными субъектами специально-криминологического воздействия являются государственные, в том числе правоохранительные, органы. Целью специально-криминологической профилактики выступает локализация, нейтрализация и

устранение общественной опасности лиц, совершивших преступления, и лиц с социально отклоняющимся поведением.

В связи с этим, представляется необходимым остановиться именно на специальных мерах предупреждения компьютерной преступности (правовых, духовно-культурных, организационно-управленческих, технических и криминалистических). К специальным правовым мерам предупреждения компьютерных преступлений можно отнести следующие:

1. Совершенствование действующего уголовного законодательства. Например, необходимо законодательное закрепление ряда юридических понятий, содержащихся в диспозициях ст. 272–274 УК РФ, а именно: «компьютерная программа», «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации», «средства хранения, обработки или передачи охраняемой компьютерной информации», поскольку указанные юридические термины законодательно нигде не определены, а разъяснения Пленума Верховного Суда РФ на данный счет отсутствуют.

2. Совершенствование судебной практики по уголовным делам о компьютерных преступлениях в Российской Федерации. До сих пор отсутствуют разъяснения Пленума Верховного Суда РФ о практике рассмотрения судами уголовных дел по преступлениям в сфере компьютерной информации, что негативно сказывается на следственно-судебной практике и единообразии применения уголовно-правовых норм правоохранительными органами.

3. Активизация и совершенствование международно-правового сотрудничества в сфере предупреждения компьютерных преступлений и борьбы с ними. Учитывая транснациональный и трансграничный характер рассматриваемых преступлений, большое значение приобретает вопрос взаимодействия правоохранительных органов России и зарубежных стран в сфере противодействия компьютерной преступности.

4. Совершенствование информационного законодательства РФ. Авторы полагают возможным принятие федерального закона о страховании информационных рисков, который бы закреплял страхование компьютерной информации, а также средств ее хранения, обработки и передачи, информационно-телекоммуникационных сетей и оконечного оборудования от несанкционированного уничтожения, блокирования, модификации либо копирования

В качестве специальных духовно-культурных (идеологических) мер противодействия компьютерным преступлениям предлагается:

1.Активизировать деятельность средств массовой информации по предупреждению компьютерных преступлений.

2. Обратить внимание на правовое воспитание молодежи. По мнению авторов, проводя правовую пропаганду и правовое просвещение среди учащихся и студентов технических образовательных учреждений — будущих программистов, сетевых администраторов и специалистов в области защиты информации, информируя их о действующем уголовном законодательстве и ответственности за указанные противоправные деяния, можно снизить риск появления компьютерных преступников в среде технических специалистов, поскольку, как показывает практика, достаточно большое количество хакеров появляется в молодежной среде технического «андеграунда».

К специальным организационно-управленческим и техническим мерам предупреждения компьютерных преступлений можно отнести следующее:

1. Подготовка специалистов по специальностям «Информационная безопасность», «Защита информации и информационно-телекоммуникационных сетей» в высших учебных заведениях МВД, ФСБ, МО РФ и др. с целью дальнейшего комплектования правоохранительных органов профессиональными и компетентными сотрудниками. При этом следует также осуществлять повышение квалификации и профессорско-преподавательского состава вышеуказанных вузов, включая проведение ста-

жировок, обмена опытом, мастер-классов, семинаров в соответствующих образовательных учреждениях за рубежом, а также в российских и иностранных компаниях, занимающихся информационной безопасностью, защитой информации, разработкой антивирусного программного обеспечения и т.п.

2. Создание в технических вузах, а также в вузах МВД, ФСБ, МО РФ научно-исследовательских лабораторий по разработке и модификации программных систем компьютерной защиты с правом реализации (продажи) своей продукции заинтересованным физическим и юридическим лицам. Работа в лабораториях должна проводиться как в научных, так и в коммерческих целях на договорной основе, в том числе для государственных и муниципальных нужд.

3. При технических образовательных учреждениях, специализирующихся на подготовке специалистов по информационной безопасности, следует создать курсы обучения и повышения квалификации для сотрудников служб безопасности банков, предприятий, учреждений либо заинтересованных компьютерных пользователей.

4. В трудовых договорах (контрактах) лиц, работающих в корпоративной компьютерной системе или информационно-телекоммуникационной сети либо имеющих доступ к ней, нужно предусмотреть положение о персональной ответственности данных лиц за разглашение конфиденциальных сведений о системе защиты служебной компьютерной сети или передачу служебных паролей и логинов третьим лицам (уголовной или иной юридической ответственности, в зависимости от тяжести наступивших последствий или угрозы их наступления).

5. С целью совершенствования систем защиты компьютерной информации в государственных и муниципальных организациях необходимо возложить на руководителей или иных уполномоченных лиц персональную обязанность осуществлять контроль за установкой и постоянным обновлением

антивирусного программного обеспечения, а также иных систем компьютерной защиты.

6. Требуется тесное взаимодействие органов прокуратуры, органов внутренних дел (отделов «К»), органов Федеральной службы безопасности со средствами массовой информации при предупреждении и раскрытии преступлений в сфере компьютерной информации. Анализ правоприменительной практики показывает эффективность такого взаимодействия, тем более что основные формы сотрудничества правоохранительных органов и средств массовой информации давно уже апробированы и активно используются.

7. Создание в Российской Федерации национальной операционной системы для компьютерных устройств, а также общенациональной компьютерной системы фиксации, анализа и учета преступлений в сфере компьютерной информации и компьютерных преступников (разработку таких систем можно поручить российским компаниям: «Лаборатория Касперского», Dr. Web, Group-IB).

К криминологическим мерам предупреждения преступлений в сфере компьютерной информации можно отнести:

1. Совершенствование уголовно-процессуального законодательства.

2. Создание новых и совершенствование существующих методик выявления компьютерных преступлений с привлечением специалистов в области информационной безопасности (например, вышеуказанных специалистов компаний «Лаборатория Касперского», Dr. Web, Group-IB).

3. Обобщение и анализ юридической практики Прокуратурой РФ, СК РФ, МВД РФ, ФСБ РФ, МО РФ для дальнейшей выработки методических рекомендаций по вопросам раскрытия и расследования компьютерных преступлений.

4. Создание во всех экспертно-криминалистических центрах МВД, ГУВД, ОВД отделов компьютерных экспертиз и технологий для производст-

ва необходимых судебно-компьютерных экспертиз, выдачи заключений и справок заинтересованным лицам.

5. Совершенствование подготовки экспертов-криминалистов, осуществляющих судебно-компьютерные экспертизы, на базе единого учебного центра[1].

Особое внимание следует обратить на технические меры

Деление средств защиты информации достаточно условно, так как на практике очень часто они и взаимодействуют, и реализуются в комплексе в виде программно-аппаратных модулей с широким использованием алгоритмов закрытия информации.

В особую группу выделяются аппаратные средства защиты ЭВМ и коммуникационных систем на их базе.

Аппаратные средства защиты применяются как в отдельных ПЭВМ, так и на различных уровнях и участках сети: в центральных процессорах ЭВМ, в их оперативных ЗУ (ОЗУ), контроллерах ввода-вывода, внешних ЗУ, терминалах и т. д.

Одной из мер аппаратной защиты ЭВМ и информационных сетей является ограничение доступа к оперативной памяти с помощью установления границ или полей. Для этого создаются регистры контроля и регистры защиты данных. Применяются также дополнительные биты четности — разновидность метода кодового резервирования.

Для обозначения степени конфиденциальности программ и данных, категорий пользователей используются биты, называемые битами конфиденциальности (это два-три дополнительных разряда, с помощью которых кодируются категории секретности пользователей, программ и данных).

[1] Пархоменко С.В., Евдокимов К.Н. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы // Криминологический журнал Байкальского государственного университета экономики и права. 2015. Т. 9. № 2. С. 265–276.

Программы и данные, загружаемые в ОЗУ, нуждаются в защите, гарантирующей их от несанкционированного доступа. Часто используются биты четности, ключи, постоянная специальная память. При считывании из ОЗУ необходимо, чтобы программы не могли быть уничтожены несанкционированными действиями пользователей или вследствие выхода аппаратуры из строя. Отказы должны своевременно выявляться и устраняться, чтобы предотвратить исполнение искаженной команды ЦП и потери информации.

Аппаратные средства защиты применяются и в терминалах пользователей. Для предотвращения утечки информации при подключении незарегистрированного терминала необходимо перед выдачей запрашиваемых данных осуществить идентификацию (автоматическое определение кода или номера) терминала, с которого поступил запрос. В многопользовательском режиме этого терминала идентификации его недостаточно. Необходимо осуществить аутентификацию пользователя, то есть установить его подлинность и полномочия. Это необходимо и потому, что разные пользователи, зарегистрированные в системе, могут иметь доступ только к отдельным файлам и строго ограниченные полномочия их использования.

Аппаратные средства защиты информации — это различные технические устройства, системы и сооружения, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа.

Программные средства защиты

Под программными средствами компьютерной техники понимаются объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения.

Рассмотрим несколько направлений применения программных средств защиты:

1. Идентификации технических средств, файлов и аутентификации пользователей. Идентификация технических средств и файлов, осуществляемая программно, делается на основе анализа регистрационных номеров различных компонентов и объектов информационной системы и сопоставления их со значениями адресов и паролей, хранящихся в защитном устройстве системы управления.

2. Обслуживания режимов обработки информации ограниченного пользования. Для разграничения обращения отдельных пользователей к вполне определенной категории информации применяются индивидуальные меры секретности этих файлов и особый контроль доступа к ним пользователей. Гриф секретности может формироваться в виде трехразрядных кодовых слов, которые хранятся в самом файле или в специальной таблице. В этой же таблице записываются идентификатор пользователя, создавшего данный файл, идентификаторы терминалов, с которых может быть осуществлен доступ к файлу, идентификаторы пользователей, которым разрешен доступ к данному файлу, а также их права на пользование файлом (считывание, редактирование, стирание, обновление, исполнение и т. д.).

3. Защита информации от несанкционированного доступа.

Для защиты от чужого вторжения обязательно предусматриваются определенные меры безопасности. Основные функции, которые должны осуществляться программными средствами, это:

- идентификация субъектов и объектов;
- разграничение (иногда и полная изоляция) доступа к вычислительным ресурсам и информации;
- контроль и регистрация действий с информацией и программами.

Процедура идентификации и подтверждения подлинности предполагает проверку, является ли субъект, осуществляющий доступ (или объект, к которому осуществляется доступ), тем, за кого себя выдает. Подобные проверки могут быть одноразовыми или периодическими (особенно в случаях про-

должительных сеансов работы). В процедурах идентификации используются различные методы:

- простые, сложные или одноразовые пароли;
- обмен вопросами и ответами с администратором;
- ключи, магнитные карты, значки, жетоны;
- средства анализа индивидуальных характеристик (голоса, отпечатков пальцев, геометрических параметров рук, лица);
- специальные идентификаторы или контрольные суммы для аппаратуры, программ, данных.

4. Защита от копирования.

Под средствами защиты от копирования понимаются средства, обеспечивающие выполнение программой своих функций только при опознании некоторого уникального некопируемого элемента.

5. Защита информации от разрушения.

Одной из задач обеспечения безопасности для всех случаев пользования ПЭВМ является защита информации от разрушения, которое может произойти при подготовке и осуществлении различных восстановительных мероприятий (резервировании, создании и обновлении страховочного фонда, ведении архивов информации и других). Так как причины разрушения информации весьма разнообразны (несанкционированные действия, ошибки программ и оборудования, компьютерные вирусы и пр.), то проведение страховочных мероприятий обязательно для всех, кто пользуется персональными ЭВМ.

Необходимо специально отметить опасность компьютерных вирусов. Многие пользователи ЭВМ (ПЭВМ) о них хорошо знают, а тот, кто с ними еще не знаком, скоро познакомится. Вирус компьютерный — небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям. Ви-

рус обычно создается для нарушения работы компьютера различными способами — от «безобидной» выдачи какого-либо сообщения до стирания, разрушения файлов.

Широкое применение для борьбы с вирусами получили резидентные антивирусы и программы-ревизоры: AIDSTEST, VDEATH, SERUM-3, ANTI-KOT, SCAN и сотни других.

6. Криптографические средства защиты.

К криптографическим методам относятся шифрование и кодирование:

- Шифрование. При передаче по электронной почте, да и просто при хранении конфиденциальной информации на компьютерах, доступ к которым имеют несколько человек, возникает потребность ограничения доступа к некоторым файлам и папкам, то есть данные шифруются перед вводом в канал связи, а расшифровываются на выходе из него[1].

В США, например, в соответствии с директивой Министерства финансов, начиная с 1984г. все общественные и частные организации были обязаны внедрить процедуру шифрования коммерческой информации по системе DES (Data Encryption Standard). Как правило, российские пользователи справедливо не доверяют зарубежным системам, взлом которых стал любимым развлечением хакеров. Однако и российские государственные системы тоже могут быть ненадежными.

- Кодирование. Существует достаточное количество программ, которые довольно надежно кодируют данные. Пожалуй, самой распространенной из них является PGP. PGP – Pretty Good Privacy - Почти Полная Приватность – это семейство программных продуктов, которые используют самые стойкие из существующих криптографических алгоритмов (алгоритмов шифрования) и

[1] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дисс. … канд. юрид. наук. М., 2005. С. 47.

предназначены для защиты приватности файлов и сообщений электронной почты в глобальных вычислительных и коммуникационных средах[1].

Завершая обзор технических мер обеспечения информационной безопасности, необходимо отметить следующее.

Разработка новых технических средств обеспечения информационной безопасности обычно сопровождается появлением новых средств несанкционированного съема информации, что в свою очередь вновь заставляет совершенствовать систему защиты. Это очень динамичный, взаимосвязанный процесс.

Специалистам по обеспечению информационной безопасности необходимо быть в курсе не только перспективных направлений развития техники защиты информации, но и совершенствования методов и средств ее несанкционированного съема. Только в этом заключается залог будущего успешного противодействия нарушениям информационной безопасности.

Таким образом подводя итоги рассмотрению вопроса стоит отметить, что система профилактических мер, направленных на предупреждение компьютерных преступлений, должна носить комплексный и многосторонний характер. Между тем, учитывая методологический подход криминологической науки, мы выделяем меры общей превенции (например, политические, экономические, социальные, научно-технические, духовно-культурные) и специальные превентивные меры (правовые, духовно-культурные, организационно-управленческие, технические, криминалистические и др.). В рамках исследования были охарактеризованы отдельные элементы предупредительных мер. Перечень мер по предупреждению компьютерной преступности может быть продолжен. Однако, вне всякого сомнения, только интегративный и комплексный подходы в применении правоохранительными органами профилактических мер могут повысить уровень информационной безопасно-

[1] Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями // Электронный ресурс. _http://www.hackzone.ru/articles/a5.html

сти России и сделать предупреждение компьютерных преступлений более эффективным. При этом не стоит забывать, что предложенные превентивные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества (органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.).

ЗАКЛЮЧЕНИЕ

Проведенное выпускное квалификационное исследование позволяет сформулировать ряд выводов и предложений, направленных на эффективную унификацию уголовно-правовых норм, устанавливающих ответственности за киберпреступления, а также на совершенствование правоприменительной практики.

1. Киберпреступления на сегодняшний день представляют большую общественную опасность. Рассмотрев отдельные виды киберпреступлений

можно прийти к выводу о том, что они это общественно опасное деяние, совершенное в электронной сфере посредством применения информационно-коммуникационных технологий, ресурсов компьютерной информации, т. е. компьютерной системы либо сети, непосредственно – в названной системе либо в сети, либо против названных объектов, посягающее в т. ч. на национальную и мировую безопасность (кибертерроризм и пр.), имущество, имущественные права (кражи, мошенничество в киберпространстве), личную безопасность (кибербуллинг, секстинг, груминг, троллинг и пр.), интеллектуальную собственность (плагиат и киберпиратство) и пр. Характерные признаки киберпреступности: общественная опасность, латентность, оперативность, удаленность, масштабность и высокая анонимность, самодостаточность, виртуальность.

2. Детерминанты киберпреступлений довольно разнообразны. Они связанны как с самими процессами, происходящими в обществе в последние годы, в частности: увеличение объема данных создаваемых, хранящихся и передаваемых по средством информационно-коммуникационных технологий; тенденция к переходу к оплате от наличных денежных средств к безналичным; появление новых средств платежей, а в частности криптовалюты. Также детерминанты киберпреступности напрямую связаны с слабой работой правоохранительных органов в данной сфере, малочисленностью специализированных кадров по выявлению и пресечению данного вида преступлений, виктимным поведением самих потерпевших, которые предоставляют злоумышленникам свои данные, которые позволяют совершить киберпреступление, отсутствием хорошего программного обеспечения по защите данных пользователей, в том числе государственных учреждений, что приводит к возможности совершения киберпреступлений.

3. Личность киберпреступника довольно нетрадиционна и имеет свои особенности. Первая особенность, по нашему мнению, заключается в низком возрасте, так лица склонные совершать киберпреступления как правило яв-

ляются активными пользователями и отлично разбираются в различных аспектах, связанных с компьютерной техникой с самого детства. Следующей особенностью данных лиц является их скрытность, так как зачастую киберпреступники незаметны в обычной жизни и большую часть своего свободного времени проводят сидя за компьютером как правило дома, при этом обладая знаниями по скрытию следов в информационной сети они успешно меняют адреса доменов существенно усложняя задачу по своей поимке.

4. Нормативной основной противодействию киберпреступности в нашей стране являются Конституция Российской Федерации, международное законодательство, федеральные законы и различные подзаконные акты. В рамках исследования были охарактеризованы виды киберпреступлений, даны их классификации и определено их место в системе уголовного закона.

5.Предупреждение характеризуется наличием четких элементов, таких как объект, предмет и субъекты, что в своей совокупности позволяет наиболее полно подходить к выстраиванию предупредительной работы, в том числе и применительно к вопросам предупреждения наркопреступности. Применительно к объекту предупреждения рассматриваемой категории преступлений объектом предупреждения являются общественные отношения связанные с институтами собственности, коммерческих, врачебных и частных и иных видов тайн, интеллектуальной собственности, чести и достоинства граждан, которые нарушаются в следствии кибератак. Предметом же киберпреступлений, является незаконное поведение лиц, связанное с совершением киберпреступлений. Субъекты предупреждения киберпреступлений могут быть условно разделены на ряд групп, в зависимости от классификационного признака. В частности, в своем вертикале субъекты могут быть представлены на федеральном, региональной и местном уровнях. Применительно к субъектам борьбы с киберпреступлений указанная вертикаль имеет место быть, и все ее звенья выполняют отведенную ей функцию. Конечно, основными субъектами предупреждения киберпреступлений мигрантов являются правоохрани-

тельные органы, которые в пределах своей компетенции осуществляют борьбу по различным направлениям. Также существует классификация в зависимости от уровней предупреждения, а именно субъекты общего, специального и индивидуального предупреждения. В данной классификационной группе главную роль выполняют органы специального предупреждения.

6. Система профилактических мер, направленных на предупреждение компьютерных преступлений, должна носить комплексный и многосторонний характер. Между тем, учитывая методологический подход криминологической науки, мы выделяем меры общей превенции (например, политические, экономические, социальные, научно-технические, духовно-культурные) и специальные превентивные меры (правовые, духовно-куль- турные, организационно-управленческие, технические, криминалистические и др.). В рамках исследования были охарактеризованы отдельные элементы предупредительных мер. Перечень мер по предупреждению компьютерной преступности может быть продолжен. Однако, вне всякого сомнения, только интегративный и комплексный подходы в применении правоохранительными органами профилактических мер могут повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным. При этом не стоит забывать, что предложенные превентивные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества (органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации.
2. Уголовный кодекс Российской Федерации.
3. Федеральный закон от 27 июля 2006 №149 «Об информатизации, информационных технологиях и защите информации».
4. Указ Президента Российской Федерации от 02 июля 2021 №400 «Об утверждении Стратегии национальной безопасности Российской Федерации».

Монографии, учебники и учебные пособия

5. Антонян Ю.М., Еникеев М.И., Эминов В.Е. Психология преступника и расследования преступлений. – М.: Юрист, 2006.
6. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского – М.: Право и закон, 1996.
7. Гаврило Ю.В., Аносов А.В., Баранов В.В. Деятельность ОВД по борьбе с преступлениями, совершѐнными с использованием информационных, коммуникационных и высоких технологий: Учебное пособие. – М.: Академия управления МВД России, 2019. Ч. 1.
8. Гладких В.И. Криминология: учебник (бакалавриат и магистратура). – М.: Юстиция, 2019.
9. Горшенков Г.Н., Костыря Е.А., Лукичев О.В. Криминология и профилактика преступлений. – СПб., 2001.
10. Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. … канд. юрид. наук. – М., 2005.
11. Долгова А.И. Понятия советской криминологии / А.И. Долгова, Б.В. Коробейников, В.Н. Кудрявцев, В.В. Панкратов. – М., 1985.
12. Дремлюга Р.И. Интернет-преступность. – Владивосток: Изд-во Дальневосточного университета, 2008.

13. Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. – М.: Юрлитинформ, 2015.

14. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дисс. … канд. юрид. наук. – М., 2003.

15. Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дисс. … канд. юрид. наук. – Волгоград, 2008.

16. Криминология: учебник / под общ. ред. А.И. Долговой. 4-е изд., перераб. и доп. – М., 2013.

17. Криминология: Учебник / Под ред. В.Н. Кудрявцева и В.Е. Эминова. – М.: Юристъ, 2007.

18. Криминология: Учебник для вузов / Под ред. В.Н. Бурлакова, Н.М. Кропачева. – СПб., 2003.

19. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дисс. ... д-ра юрид. наук. – М., 2007.

20. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дисс. ... д-ра юрид. наук. – М.: РГБ, 2007.

21. Лунеев В.В. Курс мировой и российской криминологии: учебник. В 2 т. Т. I. Общая часть. – М.: Издательство Юрайт, 2011.

22. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дисс. … канд. юрид. наук. – М., 2013.

23. Шеслер А.В. Групповая преступность: криминологические и уголовно-правовые аспекты: дисс. д-ра юрид. наук. – Екатеринбург, 2000.

Научные публикации и статьи в иных периодических изданиях

24. Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации // Академический юридический журнал. – 2015. – № 1 (59). – С. 25–26.

25. Ализаде В.А. Волеводз А.Г. Судебная практика применения ст. 174[1] УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты // Наркоконтроль. – 2017. – № 4. – С. 9.

26. Архипцев И.Н. Некоторые аспекты противодействия и профилактики преступлений, совершаемых иностранными гражданами и лицами без гражданства в России // Научные ведомости. –2012. – № 14. – С. 45.

27. Бойко О.А., Унукович А.С. Детерминанты латентных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Юридический вестник Самарского университета. – 2020. – № 6 (3). – С. 53–59.

28. Долгиева М.М. Операции с криптовалютами : актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. – 2019. – № 4. – С. 128-139.

29. Дремлюга Р.И. Незаконный оборот наркотиков и крипторынки: угрозы и вызовы правоохранителю // Международное сотрудничество и зарубежный опыт. – 2018. – № 2. – С. 33.

30. Евдокимов К.Н. Политические факторы компьютерной преступности в России / К.Н. Евдокимов // Информационное право. – 2015. – № 1. – С. 41–47.

31. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. – 2016. – № 1 (35). – С. 22.

32. Кардава Н.В. Киберпространство как новая политическая реальность: вызовы и ответы // История и современность. – 2018. – №1-2. – С. 27-28.

33. Кобец П.Н. Современное состояние теории предупреждения преступности и ее роль в оптимизации борьбы с преступлениями // Российская юстиция. – 2012. – № 1. – С. 19.

34. Кучеров И.И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. – 2018. – № 2. – С. 17-21.

35. Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста: научный журнал. – 2013. – № 5 (10). – С. 265 - 270

36. Мирончик А.С., Суслопаров А.В. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации // Юридические исследования. – 2019. – № 9. – С. 17.

37. Номоконов В.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45–55.

38. Номоконов В.А. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. – 2013. – № 5 (10). – С. 148–160.

39. Очилов Х.Р. Некоторые суждения о проблемах квалификации хищения чужого имущества с использованием компьютерных средств в условиях нынешних судебно-правовых реформ. // Review of law sciences. – 2020. – № 4. – С. 205-210.

40. Пархоменко С.В., Евдокимов К.Н. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9. – № 2. – С. 265–276.

41. Расулиев А. Киберпреступность: причины и условия, личность преступника // Вестник юридических наук. – 2020. – № 4. – С. 12.

42. Родивилин И.П. Проблемы квалификации преступлений в сфере компьютерной информации, совершаемых с использованием дистанционного

управления банковским счетом, и их предупреждение // Пролог. – 2014. – № 2 (6). – С. 61–64.

43. Родивиллин И.П., Родивиллина В.А. Криптовалюта как объект преступления // Деятельность правоохранительных органов в современных условиях: сборник материалов XXIII Международной научно-практической конференции. В 2-х томах. – Иркутск. 2018. – С. 262- 265.

44. Сальников Е.В. Сальникова И.Н. Криптовалюта как иновация экономики терророра // Науковедение. – 2016. – № 3. – С. 33.

45. Сидоренко Э.Л. Наркотики и криптовалюта: новые криминологические тренды // Наркоконтроль. – 2018. – № 2. – С. 8-13.

46. Скляров С.В., Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Криминологический журнал Байкальского государственного университета экономики и права. – 2016. – Т. 10. – № 2. – С. 322–330.

47. Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами // Право и кибербезопасность. – 2014. – № 2. – С. 27–32.

48. Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. – 2013. – № 3. – С. 219–226.

49. Эмиров М.Б., Саидов А.Д., Рагимханов Д.А. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник Дагестанского государственного университета. – 2011. – № 2. – С. 63–66.

Интернет-ресурсы

50. Berentsen A., A Short Introduction to the World of Cryptocurrencies // Federal Reserve Bank of St. Louis Review. First Quarter 2018. 100 (1). P. 1 - 16. [Электронный ресурс] URL:

https://files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf (дата обращения: 01.02.2023г.).

51. Russo, Camila. Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now. Bloomberg. [Электронный ресурс] URL: https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now?srnd=cryptocurriences (дата обращения: 12.01.2023 г.).

52. What is Ripple? [Электронный ресурс] URL:https://www.alphr.com/cryptocurrency/1009741/what-is-ripple (дата обращения: 21.01.2023).

53. Безопасность электронного банкинга / А.М. Сычев, П.В. Ревенков, А.Б. Дудка. М., 2017. 293.

54. В «Лаборатории Касперского» отметили рост числа DDoS-атак в мире https://ria.ru/20190805/1557194818.html (дата обращения 20.01.2023).

55. Конвенция о преступности в сфере компьютерной информации (ETS № 185) (г. Будапешт, 23.11.2001) // СПС «Гарант».

56. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (проект от 29.06.2021). URL: https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_R.pdf (дата обращения: 22.01.2023).

57. Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями // Электронный ресурс. http://www.hackzone.ru/articles/a5.html.

58. Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов. М., 2003. Егоров И. Россия внесла в ООН первый проект Конвенции по борьбе с киберпреступностью // Российская газета. 2021. № 168 (8519) [Электронный ресурс] // Официальный сайт Российской газеты.

URL: https://rg.ru/2021/07/27/rossiia-vnesla-v-oon-perv yj-proekt-konvencii-po-borbe-s-kiberprestupnostiu.html (дата обращения: 22.01.2023).

59. Резолюция Генеральной Ассамблеи ООН от 27 декабря 2019 г. № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». URL: https://www.un.org/ru/ga/ (дата обращения: 22.01.2023).

60. Сорокин, А.В. Компьютерные преступления: уголовно - правовая характеристика, методика и практика раскрытия и расследования // Электронный ресурс. - http://kurgan.unets.ru/~procur/my_page.htm.

Эмпирические материалы

61. Комплексный анализ состояния преступности в Российской Федерации по итогам 2022 года и ожидаемые тенденции ее развития / М.В. Гончарова, С.А. Невский, М.М. Бабаев, Р.В. Черкасов, Е.Б. Аблиязова, Е.М. Тимошина, Г.В. Коимшиди, Г.Э. Бицадзе – М.: ФГКУ «ВНИИ МВД России», 2023. – 102 с.