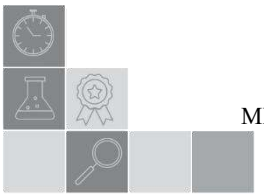
Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Учебник

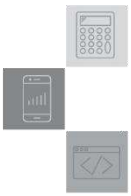
Рекомендовано Ученым советом Московского университета МВД России имени В.Я. Кикотя в качестве учебника для курсантов и слушателей



Москва

Московский университет
МВД России имени В.Я. Кикотя

2021



УДК 343.8
ББК 67.51
П83

Рецензенты:
руководитель аппарата заместителя Министра МВД России М.Г. Ваничкина кандидат экономических наук **А. В. Галянин**; заместитель начальника УУР УМВД России по Белгородской области **Р. А. Антюфеев**; начальник организационно-зонального отдела СУ УМВД России по Белгородской области **И. М. Горбатых**

Коллектив авторов:
В. В. Гончар, Т. В. Молчанова, П. В. Шмарион, А. В. Шаров, М. О. Медведева, М. М. Дайшутов, Е. А. Русскевич, Н. Н. Горач, О. В. Химичева, А. В. Тумаков, А. В. Андреев, С. П. Стащенко, Н. Т. Джафарова, А. В. Долбилов, В. Г. Любан, Д. А. Иванов, Н. В. Михайленко, Н. Е. Клишина, Д. В. Гусев, И. В. Смирнов, Д. Д. Савенкова, Д. Н. Захаров, М. В. Завьялов, Д. А. Тарасов

П83 **Противодействие преступлениям в сфере информационных технологий** : учебник / [В. В. Гончар и др.]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2021. – 332 с.
ISBN 978-5-9694-1011-4

В учебнике рассмотрены основные вопросы, связанные с особенностями противодействия преступлениям в сфере информационных технологий. Используется комплексный подход к подготовке для органов внутренних дел Российской Федерации специалистов, занимающихся противодействием преступлениям в данной сфере. Отражены административно-правовые, уголовно-правовые, уголовно-процессуальные, криминалистические, криминологические, оперативно-разыскные, организационно-правовые и организационно-технические аспекты деятельности сотрудников правоохранительных органов по противодействию указанным видам противоправной деятельности.

Учебник предназначен для курсантов и слушателей образовательных организаций МВД России, студентов образовательных учреждений юридического и технического профиля, а также преподавателей, работников правоохранительных органов, специализирующихся на противодействии противоправной деятельности в сфере информационных технологий.

УДК 343.8
ББК 67.51

ISBN 978-5-9694-1011-4

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Информационные технологии и программное обеспечение проникли во все сферы жизнедеятельности человечества. Мы используем их и на работе, и в быту, совершаем покупки и платежи, учимся, получаем, храним и делимся информацией с коллегами, друзьями и родственниками, создаем и распространяем интересные и полезные информационные продукты.

Сейчас любое техническое средство обработки информации, по сути, представляет собой микрокомпьютер, который выполняет определенную последовательность операций, зачастую имеет интерфейс взаимодействия с пользователем и, как правило, работает совместно с другими такими же средствами, обмениваясь информационными пакетами данных и образуя единое информационное пространство. При этом информация, представленная в цифровом виде, накапливается, хранится, подвергается различным модификациям и передается по каналам связи на другие устройства. В настоящее время созданы и совершенствуются информационные ресурсы практически во всех сферах деятельности человека, позволяя в кратчайшие сроки решать самые разнообразные задачи.

Вместе с тем развитие информационного пространства и использование его в благих целях активизировало противоправную деятельность ряда недобросовестных личностей и групп, которые в погоне за легкой наживой совершают различные правонарушения. Наиболее опасные из них – «компьютерные преступления», их совокупность уже имеет свое собственное, известное во всем мире название «киберпреступления», а данное явление получило наименование «киберпреступность».

При рассмотрении вопросов организации противодействия киберпреступности используется терминология, закрепленная в действующих редакциях нормативных правовых актах[1].

Содержание понятия «преступления в сфере информационных технологий» значительно шире понятия «преступления в сфере компьютерной информации». Таким образом, в учебнике главным образом изучены вопросы противодействия преступлениям в сфере информационных технологий.

Высокие темпы роста преступных посягательств в сфере информационных технологий, совершаемых в том числе против собственности, обозначили множество проблем теоретического, правового и правоприменительного характера. Как квалифицировать то или иное деяние? Как его распознать, именовать? Как найти, зафиксировать и задокументировать следы преступления в цифровом мире? Как выявить по конкретному киберпреступлению причастных лиц? Как доказать их причастность, виновность или невиновность?

Цель данной работы состоит в комплексной разработке теоретических основ противодействия преступлениям в сфере информационных технологий, в частности определении феномена киберпреступности, создании единой терминологии, понятной

---

[1] Постановление Правительства Российской Федерации от 19 августа 2017 г. № 983 «О представлении Президенту Российской Федерации предложения о подписании Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» // Правительство России [сайт]. URL: http://government.ru/all/29253/ ; распоряжение Президента Российской Федерации от 26 августа 2017 г. № 297-рп «О подписании Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201708280006 ; Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (заключено в г. Душанбе 28 сентября 2018 г.) // URL: https://cis.minsk.by/page/866.

специалистам разных сфер деятельности. На этой основе выделены проблемы правового регулирования и правоприменительной деятельности и предложены меры по их устранению.

В учебнике поставлены и решены следующие задачи:

– исследованы характерные черты информационных технологий, рассмотрены правовые основы обеспечения безопасности информации;

– изучены актуальные проблемы квалификации административных правонарушений и преступлений в сфере информационных технологий;

– дана оперативно-разыскная характеристика дистанционных хищений безналичных денежных средств граждан, совершаемых с использованием информационно-телекоммуникационных технологий;

– рассмотрены организационно-тактические и уголовно-процессуальные аспекты расследования преступлений в сфере информационных технологий;

– раскрыты проблемные вопросы использования специальных знаний при расследовании преступлений в сфере информационных технологий;

– проведен криминологический анализ преступлений в сфере информационных технологий.

Учебник предназначен для преподавателей и курсантов, слушателей, студентов образовательных учреждений юридического и технического профиля, обучающихся по следующим специальностям: 40.05.01 – Правовое обеспечение национальной безопасности; 40.05.02 – Правоохранительная деятельность; 40.05.03 – Судебная экспертиза; 10.05.01 – Компьютерная безопасность; 10.05.05 – Безопасность информационных технологий в правоохранительной сфере; 37.05.02 – Психология служебной деятельности; 38.05.01 – Экономическая безопасность; 44.05.01 – Педагогика и психология девиантного поведения, –

а также направлениям подготовки: 40.02.02 – Правоохранительная деятельность; 40.03.01 – Юриспруденция; 40.04.01 – Юриспруденция; 40.07.01 – Юриспруденция.

Учебник также может быть полезен для сотрудников правоохранительных органов, специализирующихся на противодействии противоправной деятельности в сфере информационных технологий.

ГЛАВА 1. Характеристика основных информационных технологий

§ 1.1. Понятие и виды информационных технологий

В настоящее время процессы цифровизации общества образуют значительное количество межотраслевых институтов права, которые постоянно прогрессируют в научной среде. Возникает множество научных трудов на данную тематику, которые разобщены. Отсутствует общее понимание регулирования данных общественных отношений, но при этом межотраслевые институты права считаются сформированными в научном обществе.

Процессы цифровизации связаны с обозначением актуальности того или иного продукта цифровизации общества – предложением нового продукта для цифровых правоотношений в обществе, что не всегда своевременно отражается в научных трудах цивилистов, в нормативных правовых актах на законодательном уровне.

По мнению Е. В. Евтеевой: «В зависимости от технических мощностей и возможностей, которые имеются, обществом применяются и соответствующие юридические требования к ним»[1]. С научным мнением Е. В. Евтеевой следует частично согласиться, что в правовом обществе любой научно-технический рывок (процесс) неизменно приходит к соответствующему правовому регулированию.

Исходя из этого, необходимо иметь понимание того, что каждый продукт цифровизации общества технически связан с вопросом рассмотрения информационных технологий.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

---

[1] Евтеева Е. В. Информационно-техническое обеспечение информационных технологий // Вестник ВУиТ. 2015. № 2 (24). URL: https://cyberleninka.ru/article/n/informatsionno-tehnicheskoe-obespechenie-informatsionnyh-tehnologiy.

(ред. от 02.07.2021)[1] (далее – Федеральный закон «Об информации, информационных технологиях и о защите информации») является одним из основных нормативных правовых актов, регулирующих отношения, возникающие при применении информационных технологий, осуществлении права на поиск, получение, передачу, производство и распространение информации и обеспечении защиты информации.

Информационные технологии – это процессы, методы сбора, поиска, обработки, хранения, предоставления и распространения информации, а также способы осуществления данных методов и процессов.

Подобное понимание информационных технологий содержится в законодательстве[2] и в ГОСТ 34.003–90[3], где под информационными технологиями понимаются приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных.

По назначению следует определять следующие классы информационных технологий: функциональный и обеспечивающий (рис. 1.1).

---

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/.

[2] Там же.

[3] ГОСТ 34.003–90 «Автоматизированные системы. Термины и определения» // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200006979.

Рис. 1.1. Классы информационных технологий по назначению

Выделяют следующие виды информационных технологий:

1. Автоматизация процессов.
2. Информационная технология экспертных систем.
3. Информационная технология поддержки принятия решений.
4. Информационная технология обработки данных.
5. Информационная технология управления.

Следует отметить, что использование данных (информации) в том или ином обозначении, а также приумножение новой информации, которая возникает, исходя из прогрессивности общественной жизнедеятельности в технической сфере, образуют термин «научно-технический прогресс». Его необходимо в обязательном порядке смежно рассматривать и исследовать с тематикой информационных технологий.

Термин научно-технического прогресса в настоящее время понимается и рассматривается в науке информационных технологий в двух аспектах:

1. Совокупный процесс науки и техники.
2. Действующая закономерность развития материального производства.

Так, по мнению И. Г. Шестакова, понятие научно-технического прогресса рассматривается как конкретное поступательное движение техники и науки, прогрессивное развитие всех в совокупности элементов производительных сил общественного производства на основе широкого освоения внешних сил природы и познания[1].

Однако с мнением И. Г. Шестакова расходится научная позиция М. С. Гринберга, который считает, что научно-технический прогресс – это объективная и независящая, постоянно действующая закономерность развития материального производства, результатом которой является последовательное совершенствование техники, технологии и организации производства, повышение их эффективности[2].

Следует не согласится с научной позицией М. С. Гринберга, который рассматривает в своих научных исследованиях данную проблематику и приходит к следующему выводу: ключевой фактор – это системный подход к материально-технической работоспособности мощностей, что является основой и двигателем научно-технического прогресса.

В свою очередь, вполне обоснованно научное мнение И. Г. Шестакова, которое охватывает общую совокупность возникающих и существующих процессов как технических, так и наукоемких, что подтверждает понимание термина «научно-технический прогресс».

М. Е. Мазуров рассматривает проблематику научно-технического прогресса в следующих двух формах:

1. Эволюционная.
2. Революционная.

---

[1] Шестакова И. Г. Новая темпоральность цифровой цивилизации: будущее уже наступило // Научно-технические ведомости СПбГПУ. Гуманитарные и общественные науки. 2019. № 2. С. 20–29.

[2] Гринберг М. С. Научно-технический прогресс и технические преступления // Вестник ОмГУ. 2010. № 1. URL: https://cyberleninka.ru/article/n/nauchno-tehnicheskiy-progress-i-tehnicheskie-prestupleniya.

Эволюционная форма научно-технического прогресса имеет место, когда техника и технология, применяемые в производстве, совершенствуются на основе уже известных научных знаний. Примером этой формы научно-технического прогресса являются развитие и совершенствование энергии пара, электроэнергии или атома и т. д.

Революционная форма научно-технического прогресса означает переход к технике и технологии, построенных на принципиально новых научных идеях. Примером этого являются переход от ручных орудий труда к машинным, замена энергии пара на атомную или электрическую силу, применение лазерной и других современных технологий[1].

Безусловно, рассмотрение указанных форм также подтверждает понимание терминологии научно-технического прогресса.

В подтверждение позиций научных трудов Е. В. Евтеевой, И. Г. Шестакова, М. С. Гринберга, М. Е. Мазурова выступают статистические и аналитические данные, свидетельствующие о том, что аналитический сектор, который изучает развитие IT-технологий, демонстрирует в своих исследованиях значимость для всех сфер общества вопросов цифровизации и научно-технического прогресса в целом.

Согласно аналитическим исследованиям, связанным с оценкой специалистов консалтинга IDC, мировые расходы на услуги и информационные технологии в 2023 г. достигнут 2,3 трлн долл. Данные расходы в основном обеспечат цифровую трансформацию бизнеса и организаций.

Прогнозы специалистов опираются на данные о том, что на протяжении ближайших пяти лет инвестиции в этой сфере будут стабильно расти, ежегодно увеличиваясь в среднем на 17,1 %. Также отмечается, что в 2023 г. DX-инвестиции займут более

[1] Мазуров М. Е. Моделирование научно-технического прогресса // Статистика и экономика. 2015. № 5.

50 % в общемировом объеме затрат на информационные и коммуникационные технологии, в пятерку отраслей с наибольшими расходами на цифровую трансформацию войдут розничная торговля, сфера профессиональных услуг и транспортный сектор.

Среди 219 сценариев использования, выявленных IDC, наибольшие DX-инвестиции ожидаются на таких направлениях, как автономное производство, роботизированное производство и управление грузоперевозками. В то же время с точки зрения темпов роста лидировать будут такие сегменты, как виртуальные лаборатории, цифровая виртуализация и помощь горнодобывающим предприятиям. Показатели CAGR по ним ожидаются на уровне 109,5 %, 49,9 % и 41,6 % соответственно[1].

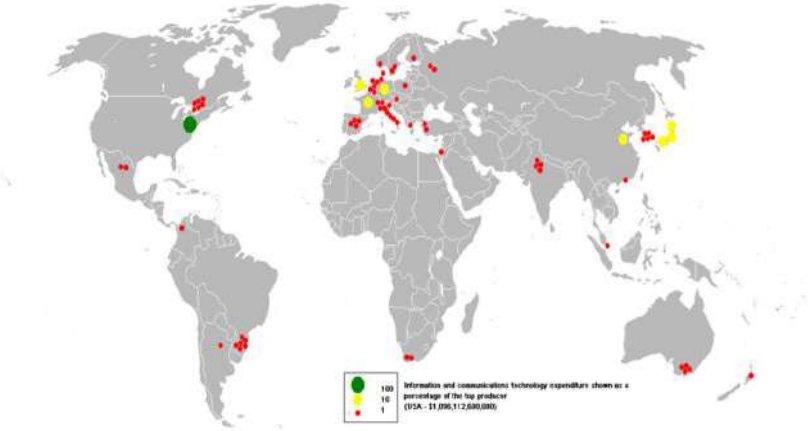


Рис. 1.2. География денежных затрат на цифровизацию общества за период с 2010 по 2020 гг.

[1] The World's Technological Capacity to Store, Communicate, and Compute Information. URL: https://bsc-consulting.ru/blog/analytics/291019/.

По мнению В. В. Шумова, вопросы рассмотрения понятия и видов информационных технологий затрагивают различные науки: технические, правовые, экономические, а также науки правоохранительной направленности[1] и безопасности государства[2].

Вопросы цифровизации общественных отношений и стремительное развитие научно-технического прогресса побуждают общество развивать все новые научные направления, в которых необходимо комплексно рассматривать сложившуюся проблематику новых явлений через призму накопившихся знаний во всех науках (технических, юридических и иных). Примером этого является формирование новой отрасли права – цифровое право, которое охватывает совокупность различных сфер человеческой жизнедеятельности, образуя при этом большое количество межотраслевых институтов права. Подобные межотраслевые институты права являются еще одним подтверждением трансформации общественных правоотношений в силу научно-технического прогресса, что полностью раскрывает проблематику рассматриваемой темы.

Огромный вклад в развитие информационных технологий вносит государственная программа, утвержденная постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”». Основной целью программы является создание широкого спектра возможностей использования информационно-коммуникационных технологий в образовательных, научных, производственных, социальных целях[3].

---

[1] Современные информационные технологии и их виды / [В. С. Володченко и др.] // Достижения науки и образования. 2018. № 18 (40). URL: https://cyberleninka.ru/article/n/sovremennye-informatsionnye-tehnologii-i-ih-vidy-1.

[2] Шумов В. В. Модель безопасности государства // УБС. 2015. № 58. URL: https://cyberleninka.ru/article/n/model-bezopasnosti-gosudarstva.

[3] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_162184/.

Указанные возможности будут доступны для любого гражданина вне зависимости от его возраста, состояния здоровья, региона проживания и т. д.

Также в развитие цифрового общества вносит вклад Национальная программа (далее – Программа), принятая в соответствии с Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», утвержденная 24 декабря 2018 г. на заседании президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам.

Данная Программа предполагает качественное переориентирование основных секторов экономики на исключительно новый формат функционирования[1]. Следует отметить, что ее реализация потребует тесного взаимодействия научно-технического общества и государства[2].

§ 1.2. Правовые основы организации и обеспечения безопасности информации

МВД России при обеспечении безопасности информации руководствуется нормативными правовыми актами, в том числе ограниченного доступа, разработанными ФСБ России, ФСТЭК России, а также ведомственными нормативными документами, регламентирующими данную деятельность.

---

[1] Гончаренко Л. П., Сыбачин С. А. Цифровизация национальной экономики // Вестник ГУУ. 2019. № 8. URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-natsionalnoi-ekonomiki.

[2] Карпова Д. Н., Проскурина А. С. Социотехнический поворот в исследовании цифровизации общества // Власть. 2020. № 1. URL: https://cyberleninka.ru/article/n/sotsiotehnicheskiy-povorot-v-issledovanii-tsifrovizatsii-obschestva.

Среди определяющих документов, регламентирующих организацию и обеспечение безопасности информации в системе МВД России, следует выделить следующие:

1. Конституция Российской Федерации – Основной закон, который содержит ряд норм, гарантирующих защиту определенной информации.

Так, в ч. 1 ст. 24 закреплено, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Для понимания данной нормы необходимо знать такие понятия, как «информация» и «частная жизнь».

Понятие информации закреплено в п. 1 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» как сведения (сообщения, данные) независимо от формы их представления.

Понятие «частная жизнь» в законодательстве не закреплено. Однако в постановлении Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (ст.ст. 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)»[1] установлено, что под собиранием сведений о частной жизни лица понимаются умышленные действия, состоящие в получении этих сведений любым способом, например, путем личного наблюдения, прослушивания, опроса других лиц, в том числе с фиксированием информации аудио-, видео-, фотосредствами, копирования документированных сведений, а также путем похищения или иного их приобретения.

Кроме того, закреплено, что под распространением сведений о частной жизни лица понимается сообщение (разглашение) их одному или нескольким лицам в устной, письменной или иной форме

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_314616/.

и любым способом (в частности, путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»).

В ч. 4 ст. 29 установлено, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется в разделе 2 Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (ред. от 11.06.2021)[1] (далее – Закон «О государственной тайне»).

В ч. 5 этой же статьи гарантируется свобода массовой информации. Установлено, что цензура запрещается.

2. Уголовный кодекс Российской Федерации (далее – УК РФ) – основной и единственный источник уголовного закона (п. 57 ст. 5 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ), единственный нормативный правовой акт, устанавливающий преступность и наказуемость деяний на территории Российской Федерации.

В УК РФ содержится ряд норм, закрепляющих уголовную ответственность за совершение общественно опасных деяний в отношении (с использованием) информации. В основном это квалифицирующие признаки, отягчающие вину лица, совершившего данное преступление. Например, в 2015–2017 гг. в информационно-телекоммуникационной сети «Интернет» получили распространение различные деструктивные виртуальные группы (наибольшую известность получила группа «Синий кит»), администраторы которых давали детям задания совершать разнообразные опасные действия вплоть до самоубийства. Государство отреагировало криминализацией данных деяний. Так, в 2017 г. была усилена ответственность за «простое» доведение до само-

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_2481/.

убийства (ч. 1 ст. 110 УК РФ), введены квалифицирующие признаки, в том числе использование информационно-телекоммуникационных сетей (включая сеть «Интернет»). В этом же году введена ст. 110.1 «Склонение к совершению самоубийства или содействие совершению самоубийства», в том числе с использованием информации или информационно-телекоммуникационных сетей (включая сеть «Интернет»).

В ст. 183 УК РФ закреплена ответственность за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Глава 28 «Преступления в сфере компьютерной информации» состоит из четырех статей:

– статья 272 «Неправомерный доступ к компьютерной информации»;

– статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;

– статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»;

– статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

В примечании к ст. 272 приводится определение компьютерной информации, как сведений (сообщения, данные), представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Наиболее важные положения данной главы рассмотрены в Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации[1] (утв. Генпрокуратурой России 15 апреля 2014 г.), в соответствии с которыми:

[1] НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/prime/doc/70542118/.

– охраняемая законом компьютерная информация – это информация, в отношении которой законом установлен специальный режим ее правовой защиты (например, государственная, банковская, коммерческая тайна, персональные данные и т. д.);

– неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты;

– уничтожение информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени;

– блокирование информации – результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, т. е. совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;

– модификация информации – внесение изменений в компьютерную информацию (или ее параметры). Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их

функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

– копирование информации – создание копии имеющейся информации на другом носителе, т.е. перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т. п.

В ст. 275 УК РФ установлена ответственность за государственную измену, т. е. «совершенные гражданином Российской Федерации… выдача иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну…».

В ст. 283 УК РФ установлена ответственность за разглашение государственной тайны.

В ст. 284 УК РФ установлена ответственность за утрату документов, содержащих государственную тайну.

В ст. 310 УК РФ установлена ответственность за разглашение данных предварительного расследования.

В ст. 311 УК РФ установлена ответственность за разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса.

В ст. 320 УК РФ установлена ответственность за разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа.

3. Кодекс Российской Федерации об административных правонарушениях (далее – КоАП РФ), где в ст.ст. 13.2–13.40 закреплен перечень административных правонарушений в области связи и информации.

Например, в ст. 13.14 КоАП РФ установлена ответственность за разглашение информации с ограниченным доступом

за исключением случаев, если разглашение такой информации влечет уголовную ответственность.

4. Закон «О государственной тайне», который регламентирует общественные отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Нормы данного закона общеобязательны для исполнения на территории Российской Федерации и за ее пределами всеми государственными органами, а также организациями, наделенными соответствующими полномочиями, органами местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

5. Федеральный закон «Об информации, информационных технологиях и о защите информации», который является определяющим в рассматриваемой области. Он регулирует отношения, возникающие:

– при осуществлении права на поиск, получение, передачу, производство и распространение информации;

– применении информационных технологий;

– обеспечении защиты информации.

В ст. 2 приводятся основные понятия, используемые в указанном федеральном законе.

В ст. 3 закреплены основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

В соответствии со ст. 5 установлены виды информации в зависимости от категории доступа к ней. Выделяют общедоступную информацию и информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

При этом отдельно выделяется класс информации, распространение которой в Российской Федерации ограничивается или запрещается.

В ст. 9 установлены требования к ограничению доступа к информации.

В соответствии со ст. 10 в Российской Федерации распространение информации осуществляется свободно при условии соблюдения требований законодательства.

6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 02.07.2021)[1] (далее – Федеральный закон «О персональных данных»), регулирующий отношения, связанные с обработкой персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях (позволяет осуществлять поиск персональных данных и (или) доступ к таким персональным данным).

В данном нормативном правовом акте рассмотрены соответствующие: основные понятия; принципы и условия обработки персональных данных; права субъекта персональных данных; меры по обеспечению безопасности персональных данных при их обработке; угрозы безопасности персональных данных; перечень лиц, ответственных за организацию обработки персональных данных; контроль и надзор за обработкой персональных данных; ответственность за нарушение требований закона.

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61801/.

7. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (ред. от 11.06.2021)[1], регулирующий отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

В законе закреплены: основные понятия; порядок использования электронной подписи; виды электронной подписи; порядок признания; использование электронной подписи; функции и обязанности удостоверяющего центра; сертификат ключа электронной подписи.

8. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2] (далее – Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»), регулирующий отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предпринима-

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_112701/.

[2] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

тели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности; российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Установлено, что государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Субъекты критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам критической информационной инфраструктуры.

Установлено, что, если объект критической информационной инфраструктуры не соответствует критериям значимости,

показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

9. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[1], в котором Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В данном нормативном правовом акте под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Установлены стратегические цели информационной безопасности в различных областях общественных отношений.

Закреплено, что система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

10. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с

[1] НПП «Гарант-сервис». URL: https://base.garant.ru/71556224/.

использованием шифровальных (криптографических) средств…»[1] определяет порядок лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), выполняемой юридическими лицами и индивидуальными предпринимателями.

11. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», устанавливающее требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.

В постановлении закреплены: актуальные угрозы безопасности персональных данных; уровни защищенность персональных данных; требования для обеспечения необходимого уровня защищенности.

12. Постановление Правительства Российской Федерации от 30 июня 2018 г. № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных,

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_128739/.

обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» (ред. от 16.08.2021)[1], где в соответствии с ч. 8 ст. 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации» утверждается состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных.

Постановлением Правительства Российской Федерации от 13 сентября 2019 г. № 1197 «О внесении изменения в состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных»[2] расширен состав сведений, размещаемых в единой биометрической системе. Дополнительно включены контактные данные физического лица (номер абонентского устройства подвижной радиотелефонной связи, адрес электронной почты).

13. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических

---

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_301465/.

[2] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_333465/.

мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»[1] раскрывает состав и содержание организационных и технических мер, необходимых для выполнения требований к защите персональных данных для установленных уровней защищенности.

14. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»[2], регулирующее отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Приводятся: перечень средств криптографической защиты информации (далее – СКЗИ); порядок эксплуатации СКЗИ; порядок контроля.

15. Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»[3] определяет порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

---

[1] НПП «Гарант-сервис». URL: https://base.garant.ru/70727118/.

[2] НПП «Гарант-сервис». URL: https://base.garant.ru/187947/.

[3] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_32924/. Режим доступа: по расписанию.

– функции органа криптографической защиты информации;

– порядок разработки инструкции по работе с конфиденциальной информацией;

– требования к личному составу органа криптографической защиты;

– порядок обращения с СКЗИ и криптоключами к ним;

– мероприятия при компрометации криптоключей;

– типовые формы журналов учета СКЗИ, технического журнала;

– требования к помещению органа криптографической защиты;

– контроль.

16. Приказ Министерства внутренних дел Российской Федерации от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации»[1] закрепляет порядок выполнения мероприятий по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, устанавливает меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также определяет обязанности должностных лиц.

В данной Инструкции не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

17. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персо-

[1] НПП «Гарант-сервис». URL: https://base.garant.ru/70230320/.

нальных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утв. руководством 8 Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432)[1] используются при разработке частных моделей угроз операторам информационных систем персональных данных, принявшим решение об использовании СКЗИ для обеспечения безопасности персональных данных.

Определено, что использование СКЗИ необходимо в следующих случаях:

– если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;

– если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

18. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[2], где приводятся структура и наполнение организационных и технических мер по обеспечению безопасности персональных данных, закреплен перечень мер по защите персональных данных в информационных системах в зависимости от уровня защищенности персональных данных.

Также представляется целесообразным указать следующие стандарты и рекомендации по стандартизации:

---

[1] Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/420336137.

[2] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_146520/.

1. ГОСТ 34.13–2018 «Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (введен в действие Приказом Росстандарта от 4 декабря 2018 г. № 1062-ст).

2. Р 1323565.1.030–2020 «Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)» (утв. и введены в действие Приказом Росстандарта от 27 февраля 2020 г. № 84-ст).

3. Р 1323565.1.025–2019 «Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами» (утв. и введены в действие Приказом Росстандарта от 29 августа 2019 г. № 593-ст).

4. ГОСТ 34.11–2018 «Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хэширования» (введен в действие Приказом Росстандарта от 4 декабря 2018 г. № 1060-ст).

5. ГОСТ 34.10–2018 «Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (введен в действие Приказом Росстандарта от 4 декабря 2018 г. № 1059-ст).

§ 1.3. Общая характеристика цифрового имущества

Развитие информационных технологий за два последних десятилетия ведет к формированию новой, так называемой цифровой реальности. Цифровые технологии проникают в сложившиеся отношения и институты (например, банковские операции в онлайн-режиме, электронные библиотеки и т. д.). Более того,

речь идет о создании новой реальности, не имеющей аналогов в прежнем мире, – интернет-вещей, цифровой экономики, криптовалюты.

В. Д. Зорькин, председатель Конституционного Суда Российской Федерации отметил, что «зарождается новое право, регулирующее отношения в контексте мира цифр и искусственного интеллекта»[1].

Цифровизация социальной жизни привела к появлению ранее неизвестных, так называемых цифровых прав. Под цифровыми правами понимаются права людей на доступ, использование, создание и публикацию цифровых произведений, на доступ и использование компьютеров и иных электронных устройств, а также коммуникационных сетей, в частности сети «Интернет».

Кроме того, Валерий Дмитриевич приходит к выводу, что «признавать и защищать цифровые права граждан от всевозможных нарушений – задача государства. Однако существующее законодательство далеко не в полной мере отвечает потребностям времени»[2].

Следует отметить, что несмотря на активную цифровизацию отечественной экономики, в настоящее время отсутствует регулирование рынка существующих в информационно-телекоммуникационной сети новых объектов экономических отношений, а именно криптовалют, токенов и т. д. На законодательном уровне в Российской Федерации данные объекты цифрового права не признаются, однако в других государствах цифровые правоотношения активно развиваются. Поскольку операции с объектами цифрового права осуществляются в сети «Интернет», доступ к ним имеют граждане многих государств, в том числе граждане Российской Федерации. Хотя оборот цифровых

[1] Зорькин В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума // Российская газета. 2018. № 7578 (115).

[2] Там же.

финансовых активов в настоящее время не соответствует требованиям безопасности в силу отсутствия в гражданском законодательстве специальных норм.

Высокие темпы цифровизации не могли не повлечь потребность в пересмотре национального гражданского законодательства. Ревизия норм гражданского права в сфере регулирования цифровых правоотношений в настоящее время особенно необходима. Во-первых, многие зарубежные государства уже сделали первые шаги к признанию таких цифровых объектов, как криптовалюты. Еще в 2014 г. служба Внутренних доходов США разъяснила, что для целей налогообложения виртуальная валюта рассматривается как имущество, а операции по выпуску криптовалюты могут быть классифицированы как размещение ценных бумаг[1].

По данным аналитического портала HowMuch[2], в 2018 г. использование биткоина разрешено в 99 из 246 стран мира. Но пока ни одна держава не посчитала необходимым назвать биткоин своей официальной валютой. При этом тенденция отказа от фиатных денег в пользу криптовалют существует в экономически благополучных странах, где малый процент транзакций происходит с использованием наличных денежных средств (Дания, Великобритания, Швеция).

В это время позиция Российской Федерации к использованию цифровых финансовых средств, в частности криптовалют, остается неоднозначной, действующее регулирование цифровых правоотношений отсутствует.

---

[1] Падалко А. Цифровые активы: новый объект гражданского права и вопросы его налогообложения при первом приближении // Rodl & Partner. 2018. май/июнь.

[2] См. подробнее о статусе биткоина в зарубежных странах: URL: https://howtobuycoin.com/bitcoin/bitcoin-official-cryptocurrency/.

Во-вторых, отечественному гражданскому законодательству необходима «цифровая прививка»[1], так как возникает необходимость в регулировании нетипичных объектов – виртуальных вещей.

Проблема определения статуса цифровых объектов является одним из актуальнейших вопросов современного гражданского права России. Промедление в регулировании этих цифровых гражданских отношений чревато не только отставанием от экономически более развитых стран, но и увеличением числа «серых» транзакций, связанных с преступной деятельностью. По мнению А. Воздвиженской, криптовалюты могут быть использованы для легализации денежных средств[2].

Также о наличии правовой неопределенности в сфере регулирования цифровых объектов свидетельствовало пристальное внимание к процедуре банкротства гражданина Ильи Царькова[3]. Решением арбитражного апелляционного суда в конкурсную массу банкрота была включена криптовалюта в количестве 0,2 биткоина. Это стало прецедентом в российской судебной практике. Ответчик ссылался на отсутствие правового регулирования криптовалют в России, однако истец, конкурсный управляющий, настаивал на включении данного объекта в конкурсную массу, иначе у должника появится возможность «прятать имущество в биткоины». Суд мотивировал свое решение тем, что в Гражданском кодексе Российской Федерации (далее – ГК РФ) перечень объектов гражданских прав не является закрытым и, следовательно, в соответствии со ст. 128 ГК РФ (объекты гражданских прав) криптовалюты можно приравнять к «иному имуществу».

---

[1] Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1 (253). URL: https://cyberleninka.ru/-article/n/pravo-v-usloviyah-tsifrovoy-realnosti.

[2] Воздвиженская А. Япония признала криптовалюты законным платежным средством // URL: https://rg.ru/2017/04/01/iaponiia-priznala-kriptovaliuty-zakonnym-platezhnym-sredstvom.html.

[3] В Москве суд завершил банкротство, в котором биткоины признали имуществом // URL: https://ria.ru/20180808/1526151217.html.

Данный пример служит хорошей иллюстрацией того, что цифровые объекты – это не метафизические категории, а реалии современной жизни, которые необходимо отразить в праве.

Кроме того, в решении суда отражено одно важное свойство цифрового объекта, которое позволяет наравне с денежными средствами и иным имуществом признавать объектом гражданского права и, следовательно, включать в конкурсную массу в процедуре банкротства. Это свойство ликвидности цифрового объекта. Ликвидность – способность актива превращаться в деньги. Ликвидность определяется скоростью трансформации актива и количеством потерь стоимости при такой трансформации. В этом прослеживается отличительная черта цифровых объектов гражданского права от объектов, хотя и имеющих цифровую форму, но отличающихся по содержанию. Например, вряд ли можно считать цифровым объектом гражданского права количество древесины, добытой в игре War Craft 3, по причине невозможности осуществить обмен и монетизировать данный ресурс. Иначе дела обстоят с крупными сетевыми играми, в которых предусмотрена возможность приобретения игровых предметов за реальные деньги.

Перед определением правового режима цифрового имущества необходимо определиться с категориальным аппаратом заявленной темы. Рассуждая о развитии гражданского права, многие цивилисты используют термины «цифровой» и «виртуальный», зачастую не проводя разграничений между этими понятиями. Обратившись к толковому словарю, отметим, что слово «виртуальный» имеет следующее значение: несуществующий, но возможный, который не имеет физического существования, а реализуется лишь в компьютерных условиях, в фантазии и т. п.[1]

Следует отметить, что для целей научного исследования цифрового имущества термин «виртуальный» необходимо тол-

[1] Gufo.me – коллекция словарей и энциклопедий. URL: https://gufo.me.

ковать как «не имеющий физического эквивалента и реализуемый в компьютерных условиях». Это означает, что объект изначально был создан в электронно-вычислительной среде и у него нет «копий» в материальном мире. Примерами виртуальных явлений в повседневной жизни могут служить: разнообразные «личные кабинеты» на интернет-сайтах, электронная почта, электронные библиотеки, виртуальная игровая валюта, виртуальная реальность в компьютерных играх и т. д. Научно-технический словарь раскрывает значение термина «цифровой» как информацию, выраженную при помощи чисел[1]. С помощью чисел возможно воспроизводить, хранить, передавать, обрабатывать любую информацию, необходимо лишь ее закодировать определенным образом. По мнению М. А. Рожковой, «цифровизация предполагает прежде всего изменение формата или формы: самым тривиальным здесь будет пример перехода организации с бумажного документооборота на электронный, требующий применения информационных технологий»[2]. Также иллюстрацией цифровых явлений могут быть: электронные полисы ОСАГО, записи в ЕГРП и т. д.

Объекты, названные «виртуальными» или «цифровыми», интуитивно воспринимаются как нечто, существующее в виде программного кода в электронно-вычислительных системах. Однако эти понятия не являются тождественными. «Виртуальный» относится к характеристике природы объекта, в то время как термин «цифровой» относится к характеристике формы выражения. Виртуальному противопоставляется реальное (материальное, физическое), цифровому – аналоговое.

Таким образом, с учетом потребности в исследовании цифрового имущества можно классифицировать имущество по двум

---

[1] Gufo.me – коллекция словарей и энциклопедий. URL: https://gufo.me.

[2] Рожкова М. А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым // URL: https://zakon.ru/blog/2018/06/13/-cifrovye_aktivy_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe.

основаниям: природа и форма представления. По природе можно разделить объекты на виртуальные и материальные, по форме представления – на цифровые и аналоговые. Виртуальные объекты находят свое выражение преимущественно в цифровой форме, однако могут существовать и в аналоговой, например мысли, фантазии, идеи и т. п.

Феноменальность термина «цифровое имущество» заключается в том, что он объединяет различные по природе происхождения объекты имущества, сходные своей цифровой формой. Следовательно, представляется логичным выделять цифровое виртуальное и цифровое физическое имущество.

К цифровому материальному имуществу относятся «уже известные гражданскому праву объекты в том случае, если они созданы не «старым», традиционным способом, а при помощи современных технологий в «новой» – электронной – форме (компьютерная анимация, электронная музыка, цифровая живопись)»[1].

К цифровому виртуальному имуществу можно отнести следующие объекты:

1. Криптовалюта. К определению понятия «криптовалюта» существует несколько подходов. В частности, Базельский Комитет по банковскому надзору раскрывает понятие «криптовалюта» через определение цифровой валюты. «Цифровая валюта (или нефиатная валюта) – это не являющийся законным платежным средством актив, существующий только в электронном виде, который может использоваться в качестве средства платежа, средства хранения, единицы учета. Цифровые валюты часто опираются на технологию распределенного регистра для записи и проверки транзакций, совершенных с использованием цифровой

[1] Рожкова М. А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым // URL: https://zakon.ru/blog/2018/06/13/-cifrovye_aktivy_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe.

валюты. Из-за использования криптографических методов подмножество цифровых валют называется „криптовалютами”»[1].

Д. С. Вахрушев и О. В. Железнов предлагают под криптовалютой понимать особую разновидность электронных денег, функционирование которых основано на децентрализованном механизме эмиссии и обращении и представляющих собой сложную систему информационно-технологических процедур, построенных на криптографических методах защиты, регламентирующих идентификацию владельцев и фиксацию факта их смены»[2].

Анализируя труды Дж. Хоспа, можно сделать вывод, что в его понимании криптовалюта – это существующая в системе блокчейн валюта, функционирующая по принципу децентрализации, безопасность оборота которой обеспечивается криптографией[3].

Основной сайт биткоина[4] не дает определение понятию «криптовалюта». Однако на основе анализа таких терминов, как «биткоин» и «цепочка блоков (блокчейн)», можно вывести следующее определение: криптовалюта – это валюта или расчетная единица, существующая в децентрализованной p2p платежной сети, которая обслуживается ее же пользователями, без центральных органов управления или посредников.

Европейский центральный банк дает следующее определение: «Криптовалюта – цифровое представление стоимости, которое

---

[1] Basel Committee on Banking Supervision Consultative Document Sound Practices: Implications of fintech developments for banks and bank supervisors. Issued for comment by 31 October 2017 August 2017 // URL: https://www.bis.org/bcbs/publ/d415.pdf.

[2] Вахрушев Д. С., Железов О. В. Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления // Вестник евразийской науки. 2014. № 5 (24). URL: https://cyberleninka.ru/-article/n/kriptovalyuta-kak-fenomen-sovremennoy-informatsionnoy-ekonomiki-problemy-teoreticheskogo-osmysleniya.

[3] Дж. Хосп. О криптовалюте просто. Биткоин, эфириум, блокчейн, децентрализация, майнинг, ICO & Co. СПб. : Питер, 2019.

[4] См.: URL: https://bitcoin.org.

в некоторых случаях может использоваться в качестве альтернативы деньгам, эмитентом которого не является центральный банк, кредитная организация»[1].

В п. 18 ст. 1 Директивы 2018/843 Европейского Парламента и Совета от 30 мая 2018 г. (так называемой 5AMLD (5 anti money laundering directive) дано следующее определение: «Криптовалюта – это цифровое представление ценности, которое не выпущено или гарантировано центральным банком либо государственным органом, необязательно связано с легально установленной валютой и не имеет правового статуса валюты или денег, но принимается физическими или юридическими лицами как средство обмена и может быть передано, сохранено и продано в электронном виде»[2].

Обобщая характерные для криптовалюты черты, с учетом аспектов, отмеченных в приведенных определениях разумно дать понятию «криптовалюта» следующую дефиницию:

Криптовалюта – существующая в обслуживаемой пользователями децентрализованной электронно-вычислительной сети виртуальная валюта, оборот которой осуществляется с помощью криптографических методов верификации права собственности, а эмиссия новых единиц является вознаграждением за поддержание работоспособности системы.

2. Виртуальные токены. В настоящее время нашло признание то, что токены, с технической стороны представляющие собой лишь запись в распределенном реестре, в юридическом смысле могут обозначать фактически любое правовое явление:

---

[1] European Central Bank. Virtual currency schemes – a further analysis. February 2015. URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[2] Директива Европейского союза 2018/843 от 30 мая 2018 г., вносящая изменения в Директиву Европейского союза 2015/849 по предотвращению использования финансовой системы для целей легализации доходов, полученных преступным путем, финансирования терроризма и вносящую изменения в Директивы 2009/138/ЕК и 2013/36/ЕС // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843.

«Феноменальность токена заключается в том, что он может отображать, что угодно»[1]. И это обстоятельство делает проблематичным отнесение всех токенов к виртуальному имуществу. Так, в некоторых случаях токены могут обозначать имущественное право на вполне материальные вещи (например, один токен может быть приравнен к одному квадратному метру жилой площади или одному килограмму моркови) или получение «реальных» услуг (например, на просмотр фильма в кинотеатре) либо означать предоставленное лицу, которое приобрело инвестиционные (security) токены, право на получение прибыли компании и т. п.

3. Доменные имена. Еще в 2001 г. при рассмотрении доменного спора относительно использования товарного знака Kodak в доменном имени kodak.ru Президиум Высшего Арбитражного Суда Российской Федерации отметил следующее: «Доменные имена фактически трансформировались в средство, выполняющее функцию товарного знака, который дает возможность отличать соответственно товары и услуги одних юридических или физических лиц от однородных товаров и услуг других юридических или физических лиц. Кроме того, доменные имена, содержащие товарные знаки или торговые наименования, имеют коммерческую стоимость»[2]. Таким образом, доменные имена с определенного момента помимо технической функции переадресации в сети «Интернет» стали использоваться для выделения (идентификации) товаров, работ, услуг или бизнеса одних производителей, продавцов и исполнителей среди аналогичных товаров, работ, услуг[3].

---

[1] Юрасов М. Защита прав инвесторов при проведении ICO блокчейн-проектов // URL: https: //zakon.ru/blog/ 2017/11/5/zaschita_prav_investorov_pri_-provedenii_ico_blokchejn-proektov.

[2] Постановление Президиума Высшего Арбитражного Суда Российской Федерации от 16 января 2001 г. № 1192/00 по делу № А40-25314/99-15-271 // URL: https://www.allpravo.ru/jurisprudence/doc2096p/instrum2097.

[3] Рожкова М. А. Права на доменное имя // Право в сфере Интернета : сборник статей / рук. авт. кол. и отв. ред. М. А. Рожкова. М. : Статут, 2018. С. 195–223. URL: https://cctld.ru/files/books/rozhkova_asp.pdf.

4. Виртуальное имущество в социальных сетях. Данный класс виртуального имущества представлен аккаунтами в социальных сетях, а также разнообразными наборами стикеров-картинок, персонализирующими настройками, которые возможно приобрести у разработчиков. Много вопросов возникает при определении правового статуса аккаунта в социальной сети: можно ли считать, что все действия, совершенные с аккаунта пользователя, совершены его владельцем; возможно ли наследование аккаунта; правомерен ли оборот аккаунтов социальных сетей и т. д. Однако, вне всякого сомнения, остается тот факт, что аккаунт может обладать экономической ценностью, например, при большой его посещаемости другими пользователями аккаунт может выполнять функцию рекламного щита, следовательно, способствовать ведению предпринимательской деятельности.

5. «Игровое имущество». Иначе дела обстоят с крупными сетевыми играми, в которых предусмотрена возможность приобретения игровых предметов за реальные деньги. В настоящее время существует множество интернет-площадок, занимающихся скупкой и перепродажей игровых предметов за реальные деньги по ценам ниже, чем у разработчика[1]. Аналогично обстоят дела со сделками по продаже доступа к аккаунтам сетевых игр: более продвинутые игроки продают доступ к своим учетным записям менее продвинутым.

Налицо осуществление сделок купли-продажи, хотя предмет данной сделки в силу своей специфики больше похож на объект интеллектуальной собственности, для реализации которого следовало бы применить договор лицензии. Однако пользователь, решивший реализовать игровой предмет другому лицу, не является обладателем исключительного права на данный предмет, следовательно, заключить подобный договор он также не может.

---

[1] См. подробнее о купле-продаже игровых предметов: URL: https://lis-skins.ru.

ГЛАВА 2. Актуальные проблемы квалификации административных правонарушений в сфере информационных технологий

§ 2.1. Общая характеристика административных правонарушений, совершаемых в сфере информационных технологий

Сфера информационных технологий как самостоятельный структурный элемент современной действительности сложилась сравнительно недавно. Фактором, обусловившим возникновение и стремительное развитие данной сферы, послужили создание компьютерной техники и повсеместное внедрение электронно-вычислительных средств в повседневную деятельность.

Параллельно с этим частым явлением в сфере информационных технологий стало совершение различных правонарушений, влекущих определенные негативные последствия, в связи с чем возникла необходимость установления административной ответственности за правонарушения в области связи и информации.

Можно говорить о том, что обеспечение информационной безопасности является одним из приоритетных направлений государственной политики и деятельности органов внутренних дел.

Отметим, что состояние информационной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных правонарушений в отношении объектов информационной инфраструктуры[1].

[1] По данным Совета Безопасности Российской Федерации, в 2016 г. было зафиксировано около 52,5 млн кибератак на вэб-сайты госорганов (в 2015 г. – 14,4 млн). Цель большинства атак – получение информации ограниченного доступа и нарушение функционирования технических средств.

По этой причине основными направлениями ее обеспечения являются:

– повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования;

– развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления;

– повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической инфраструктуры;

– повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия данным правонарушениям.

Прежде чем рассматривать особенности квалификации административных правонарушений в сфере информационных технологий, уместно отметить отдельные теоретические аспекты науки административного права, касающиеся процесса квалификации.

Квалифицировать административное правонарушение – значит установить тождество между признаками административного правонарушения, закрепленного в административно-правовой норме, и признаками совершенного противоправного деяния.

Следовательно, под квалификацией административных правонарушений понимается установление соответствия признаков совершенного деяния признакам конкретного состава административного правонарушения, предусмотренного соответствующей статьей КоАП РФ. В случае совершения административных правонарушений в области связи и информации это напрямую относится к составам, закрепленным преимущественно в гл. 13 КоАП РФ «Административные правонарушения в области связи и информации». Однако к вышеуказанной группе административных правонарушений следует относить и ч. 1 ст. 14.1.1 «Незаконные организация и проведение азартных игр», так как объективная сторона данного правонарушения предусматривает

организацию и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны с использованием информационно-телекоммуникационных сетей (в том числе сети «Интернет») или средств связи (в том числе подвижной связи).

При этом квалификация административных правонарушений осуществляется на всех стадиях производства по делам об административных правонарушениях. Исключение может составлять стадия исполнения постановлений по делам об административных правонарушениях. Нормы, регламентирующие производство по делам об административных правонарушениях и исполнение постановлений, содержатся в ряде глав КоАП РФ.

Процесс квалификации административных правонарушений в сфере информационных технологий характеризуется рядом особенностей, которые во многом обусловлены свойствами информации и в целом информационного пространства как сферы совершения правонарушений.

Квалификация по объективной стороне предполагает сопоставление признаков совершенного деяния с его характеристикой, содержащейся в соответствующей статье КоАП РФ.

Однако формулировка некоторых статей КоАП РФ не содержит четких описаний всех действий, образующих объективную сторону административного правонарушения. В них иногда указываются весьма общие признаки возможных противоправных деяний.

Решая в подобных случаях вопрос о признании или непризнании совершенных конкретных действий соответствующими признакам объективной стороны состава, правоприменитель должен, прежде всего, осуществить семантическое, логическое толкование термина, указанного в законе, чтобы понять, какие действия охватываются этим термином. Если же в диспозиции статьи названы лишь противоправные последствия, то правоприменитель выясняет, какими вообще действиями они могут быть

вызваны. В особенности это относится к административным правонарушениям в сфере информационных технологий, поскольку при изучении механизма совершения данных правонарушений и установлении виновных лиц крайне важным представляется точное знание и владение специальной терминологией, используемой в сфере информационных технологий.

Признаки объективной стороны находят свое выражение в общественно опасных деяниях. При этом следует отметить, что именно негативные последствия, характер и тяжесть причиненного вреда являются той гранью, с помощью которой условно проводится отграничение административной ответственности от уголовной.

Квалификация по объективной стороне в ряде случаев предполагает установление соответствия реального последствия совершенного деяния его признакам, содержащимся в составе. Такая необходимость возникает при квалификации по признакам материальных составов, где последствия деяния включены в число конструктивных признаков, подлежащих оценке и сопоставлению. Заметим, что все составы административных правонарушений указанной группы являются формальными, что не требует наличия наступления последствий.

При квалификации деяний по признакам административных правонарушений, в составах которых содержится указание на такие признаки объективной стороны, как место, время, способ совершения деяния, необходимо их исследование и сопоставление с признаками соответствующего состава, что в случае совершения правонарушений в сфере информационных технологий представляет особую сложность.

Квалификация по объекту также грозит определенными трудностями. Исследуя фактические обстоятельства совершенного деяния, правоприменитель чаще всего лишен возможности непосредственного восприятия его объекта. Сложность установления непосредственного объекта квалифицируемого деяния в ряде

случаев обусловлена отсутствием четкой правовой характеристики родовых и непосредственных объектов правонарушений.

В некоторых ситуациях определяющее значение для квалификации административного правонарушения имеет предмет посягательства. В случае совершения административных правонарушений в сфере информационных технологий информация может выступать не только в качестве объекта противоправного посягательства, но и быть предметом.

Указание в административно-правовой норме на предмет или характеристики предмета правонарушения нередко служит критерием разграничения одного состава административного правонарушения в сфере информационных технологий от другого.

Среди факторов, имеющих большое значение для установления административной ответственности, можно выделить следующие:

1. Широкий состав субъектов, к которым может быть применена административная ответственность: физические лица, должностные лица, юридические лица, органы государственной власти и органы местного самоуправления.

2. Наличие ситуаций, при которых от правонарушения может пострадать неопределенное количество субъектов (например, в результате рассылки спама или иной ложной информации), а также ситуаций, при которых сложно установить источник опасности и конкретных правонарушителей (в результате распространения компьютерных вирусов).

3. Сложный механизм установления времени совершения административного правонарушения в связи с возможностью его совершения в разных географических точках и часовых поясах информационного пространства.

4. Сложность определения места административного правонарушения, учитывая, что оно фиксируется не на территории

определенного государства и вне сферы его юрисдикции, а в информационном пространстве без границ, которое предоставляет интернет.

5. Сложность фиксации факта административного правонарушения с учетом скорости обращения документированной информации в виртуальном пространстве информационных коммуникаций.

6. Отдельные сложности при установлении подлинности и сохранности электронного документа.

7. Несоответствие санкций, предусмотренных административным законодательством за правонарушения в информационной сфере, нанесенному ущербу в результате совершения правонарушений в данной сфере.

8. Высокая значимость фактов пренебрежения или неверного соблюдения правил безопасности пользователями в сфере информационных технологий.

9. Сложности в разграничении уголовной и административной ответственности.

Следовательно, такие обстоятельства, как установление места и времени совершения административного правонарушения, выявление следов при совершении подобных правонарушений, непосредственно влияют на процесс квалификации административных правонарушений в сфере информационных технологий.

Можно говорить о том, что ключевым признаком административных правонарушений в сфере информационных технологий является совершение противоправных деяний именно в связи с применением информационных систем, информационных технологий и других элементов информационной инфраструктуры.

Особенности квалификации административных правонарушений в сфере информационных технологий в первую очередь связаны со спецификой объекта, на который посягает данный тип правонарушений.

Так, информация, по В. Г. Афанасьеву, обладает специфичной правовой природой, которая проявляется в следующем:

1. Информация представляет собой такое знание, которое необходимо и в котором есть потребность.

2. Актуальной информацией является не всякое знание или сообщение, а только то, которое было принято и используется для ориентирования и оказания воздействия на тот или иной объект управления.

3. От информации необходимо отличать информационные данные, т. е. всевозможные сообщения, сведения, знания, которые могут храниться, перерабатываться, передаваться, но получают характер информации только тогда, когда используются в управлении[1].

А. Б. Венгеров, в свою очередь, изучая вопросы административно-правового регулирования сферы информации, пришел к выводу о том, что для права имеют значение такие признаки информации, как:

1) определенная самостоятельность информации по отношению к своему носителю;

2) возможность многократного использования одной и той же информации;

3) неисчерпаемость информации при ее потреблении;

4) возможность сохранения информации;

5) способность информации к интеграции, накоплению и сжатию;

6) системность изложения[2].

Вместе с тем информация выступает как объект административных правоотношений, складывающихся в информационном пространстве.

---

[1] Афанасьев В. Г. Социальная информация и управление обществом. М. : Политиздат, 1975.

[2] Венгеров А. Б. Право и информация в условиях автоматизации управления. Теоретические проблемы : автореф. дис. ... д-ра юрид. наук. М., 1975.

По мнению В. В. Крылова[1], административные правоотношения в сфере информационных технологий – это правоотношения, возникающие при:

– формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;

– создании и использовании информационных технологий и средств их обеспечения;

– защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Рост правонарушений с использованием информационных технологий, совершаемых в сети «Интернет», обусловлен объективными обстоятельствами.

Так, существующие правила эксплуатации киберпространства позволяют обеспечивать анонимность действий всех пользователей сети «Интернет», в результате чего существенно осложняется идентификация пользователей и оборудования, используемого правонарушителями.

Как показывает практический опыт, большинство правонарушений с использованием информационных технологий совершается с использованием вредоносных программ, а также специфических возможностей операционных систем, позволяющих получить удаленный доступ к информационным ресурсам, находящимся под защитой и охраняемым нормами права.

Наглядно негативные последствия от правонарушений в сфере информационных технологий можно представить в цифрах.

Например, по данным ПАО «Сбербанк», потери экономики страны в 2021 г. могут составить около 7 трлн руб., что существенно выше аналогичных показателей 2020 г.[2]

---

[1] Крылов В. В. Основы криминалистической теории расследования преступлений в сфере информации. М. : МГУ, 1998.

[2] См. подробнее: URL: https://tass.ru/ekonomika/8761953.

Вместе с тем расширение сферы безналичных расчетов повлекло за собой возникновение своеобразной криминальной индустрии, необходимой для совершения несанкционированных операций по переводу денежных средств, в том числе с использованием платежных карт[1].

Противоправные информационные технологии постоянно совершенствуются, становясь доступными широкому кругу лиц, которые могут не обладать достаточными познаниями в области информационных технологий. Повышение доступности мошеннических схем и инструментов для их реализации ожидаемо влечет за собой рост числа незаконных транзакций. Так, в 2016 г. количество несанкционированных операций с использованием платежных карт выросло на 13,8 % (с 260 тыс. до 296 тыс.), а объем ущерба составил 1,08 млрд (1,15 млрд) руб. В подавляющем большинстве несанкционированные операции производятся посредством сети «Интернет» и мобильных устройств, в том числе интернет-банкинга.

Чаще всего (в 93 % случаев) такие операции означают использование электронных средств платежа (далее – ЭСП) «без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности аутентификационной информации». В качестве причин значительной части указанных операций называются воздействие вредоносного кода и побуждение владельца ЭСП к совершению операции путем обмана и злоупотребления доверием. Общее число несанкционированных операций по счетам юридических лиц сократилось с 1 074 до 717, а их объем – с 3,79 до 1,89 млрд руб. Основной целью киберпреступников являются не крупные корпорации, а предприятия малого и среднего бизнеса. При этом, если средний объем несанкционированной транзакции по платежным картам составлял 3,7 тыс. руб., то по корпоративным счетам – уже 2,7 млн.

[1] Рожков Р. Киберпреступность вычли из ВВП // Коммерсант. 2016. 14 апр.

Как показало исследование Лаборатории Касперского, в 2017 г. треть российских компаний (36 %) хотя бы раз подверглась DDoS-атакам[1] (в 2016 г. – 17 %). Среди микропредприятий пострадали 37 %, компаний среднего и малого бизнеса – 31 %, а больших корпораций – 39 %. При этом каждый пятый пострадавший (21 %) признался, что атака привела к значительному снижению производительности сервисов компании, а у 8 % произошел сбой транзакций и процессов. Помимо непосредственного ущерба, кибератака может таить в себе и скрытую угрозу. Каждая третья компания (35 %) полагает, что атаки были отвлекающим маневром. Почти в половине случаев (47 %) кибератака сопровождалась утечкой или кражей данных, 43 % случаев – взломом корпоративной сети, а в 41 % – включала заражение вредоносным программным обеспечением. У трети пострадавших (31 %) произошло еще и прямое хищение финансовых средств.

DDoS-атака имеет место в случаях, при которых на сервер компании или банка одновременно приходит очень много запросов от разных компьютеров, контроль над которыми предварительно получили злоумышленники. От такого массового наплыва запросов сайт перестает работать, в результате чего организация получает не только финансовый, но и репутационный ущерб.

С целью минимизации масштабов киберугроз был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», который установил организационно-правовые основы обеспечения безопасности критической инфраструктуры в целях ее устойчивого функционирования, определил права и обязанности ее владельцев, а также полномочия государственных органов в указанной сфере.

Таким образом, можно говорить о том, что квалификация административных правонарушений в сфере информационных

[1] Форма № 10-а Судебного департамента при Верховном Суде Российской Федерации «Отчет о числе осужденных по всем составам преступлений Уголовного кодекса РФ» за 2013 – I полугодие 2017 г.

технологий является важнейшим элементом деятельности по обеспечению информационной безопасности, а также по обеспечению возможности безопасного обмена какими-либо данными при помощи цифровых технологий в электронной среде всеми пользователями.

При этом правильная квалификация административных правонарушений – залог обеспечения правопорядка в сфере информационных технологий, что с учетом реалий XXI в. представляется весьма актуальным.

В ходе административно-правовой квалификации систематизация признаков оцениваемого деяния осуществляется в соответствии с элементами состава административного правонарушения, а именно относящимися к объекту, объективной стороне, субъекту и субъективной стороне административного правонарушения.

При этом параллельно осуществляется сопоставление выявленных и сгруппированных признаков деяния с соответствующими элементами составов административных правонарушений.

На основе сформулированной в сознании правоприменителя при анализе фактических обстоятельств дела модели административного правонарушения из всего нормативного материала выделяется конкретный состав административного правонарушения, под признаки которого подпадает определенное правонарушение.

Таким образом, основным содержанием процесса квалификации административных правонарушений в сфере информационных технологий является сопоставление признаков совершенного деяния с признаками состава административного правонарушения, предусмотренного КоАП РФ.

Очевидно, что сопоставить совокупность всех признаков в большинстве случаев представляется затруднительным. В связи с этим квалификация правонарушений в сфере информационных технологий должна осуществляться последовательно, по элементам состава.

В первую очередь административные правонарушения квалифицируются по признакам объективной стороны. Первоочередной оценке и последующему сопоставлению с признаками состава административного правонарушения подлежат признаки, характеризующие деяние.

Основными отличительными признаками административного информационного правонарушения являются следующие: то, что объектом посягательства является порядок государственного управления в информационной сфере, связанный с обеспечением прав и свобод человека и гражданина, общественного порядка и нравственности, установленного порядка государственной власти и безопасности; противоправность как признак, подчеркивающий направленность деяния на нарушение установленных нормами административного наказания правил поведения.

Таким образом, административное информационное правонарушение можно определить как общественно опасное, противоправное, виновное деяние (действие или бездействие) деликтоспособного лица, посягающее на установленный порядок государственного управления в информационной сфере и (или) с использованием информационных средств и информационных технологий либо иных видов информационной деятельности.

Исходя из рассмотренных предпосылок можно выделить ряд составов из КоАП РФ, являющихся административными правонарушениями, совершаемыми в цифровом пространстве:

– статья 13.11 «Нарушение законодательства Российской Федерации в области персональных данных»;

– статья 13.12 «Нарушение правил защиты информации»;

– статья 13.13 «Незаконная деятельность в области защиты информации»;

– части 5, 7, 8, 9, 10, 11 ст. 13.15 «Злоупотребление свободой массовой информации»;

– часть 2 ст. 13.18 «Воспрепятствование уверенному приему радио- и телепрограмм и работе сайтов в сети „Интернет”» (воспрепятствование работе сайтов в сети «Интернет», в том числе официальных сайтов органов государственной власти или органов местного самоуправления, за исключением случаев ограничения доступа к сайтам в сети «Интернет» на основании решения суда или решения уполномоченного федерального органа исполнительной власти, либо совершение действий, направленных на заведомо незаконное ограничение доступа к таким сайтам);

– статья 13.27 «Нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети „Интернет”»;

– статья 13.27.1 «Нарушение требования о размещении на территории Российской Федерации технических средств информационных систем»;

– статья 13.31 «Неисполнение обязанностей организатором распространения информации в сети „Интернет”»;

– статья 13.33 «Нарушение обязанностей, предусмотренных законодательством Российской Федерации в области электронной подписи»;

– статья 13.34 «Неисполнение оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети „Интернет”, обязанности по ограничению или возобновлению доступа к информации, доступ к которой должен быть ограничен или возобновлен на основании сведений, полученных от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций;

– статья 13.37 «Распространение владельцем аудиовизуального сервиса информации, содержащей публичные призывы

к осуществлению террористической деятельности, материалов, публично оправдывающих терроризм, или других материалов, призывающих к осуществлению экстремистской деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности»;

– статья 13.40 «Неисполнение обязанностей оператором поисковой системы»;

– часть 1 ст. 14.1.1 «Незаконные организация и проведение азартных игр».

Нельзя не сказать о том, что установление административной ответственности за правонарушения в сфере информационного пространства невозможно без знаний других отраслей юридической науки, а именно информационного и уголовного права. Это объясняется особенностями самого объекта рассматриваемых нами правонарушений – информации, поскольку грань, разделяющая различные виды ответственности, достаточно тонкая, но в совокупности существующие меры как уголовно-правового, так и административно-правового характера направлены на обеспечение информационной безопасности.

Отметим, что благодаря механизмам, предоставляемым административным законодательством, существует возможность пресекать правонарушения в сфере информационных технологий достаточно эффективными способами, среди которых наиболее частым в судебной практике стало блокирование сайта в сети «Интернет», контент которого не отвечает требованиям действующего законодательства, а также обладает признаками, позволяющими считать его экстремистским. В последующем уполномоченными лицами могут быть применены такие меры административного реагирования, как ограничение доступа к копии заблокированного сайта, приостановление деятельности сетевого издания. Подобные превентивные меры способствуют защите различных категорий пользователей информационных систем от неправомерной информации, способной причинить существенный вред.

§ 2.2. Юридический анализ административных правонарушений в сфере информационных технологий

Подавляющее большинство административных правонарушений в области информационных технологий объединены в гл. 13 КоАП РФ. При этом надо заметить, что данная глава объединяет в себе две относительно самостоятельные группы правонарушений, такие как правонарушения в области связи и правонарушения в области информации.

По мнению Е. В. Евсиковой, наличие административной ответственности является одним из основных правовых средств сдерживания роста самых распространенных и разнообразных видов правонарушений. Иными словами, административная ответственность служит своеобразным барьером на пути совершения масштабных противоправных деяний в области информационных технологий.

Одной из наиболее часто применимых статей в области информации является ст. 13.15 КоАП РФ «Злоупотребление свободой массовой информации».

Объектом административного правонарушения, предусмотренного ст. 13.15 КоАП РФ, являются общественные отношения, складывающиеся в сфере свободы массовой информации.

Объективная сторона злоупотребления свободой массовой информации выражается в совершении действий, перечисленных в чч. 1–11 ст. 13.15 КоАП РФ, которые по своему содержанию во многом аналогичны формам злоупотребления свободой массовой информации, закрепленным в ст. 4 Закона Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»[1].

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_1511/.

К субъектам административного правонарушения, предусмотренного ст. 13.15 КоАП РФ, можно отнести достаточно большое количество лиц, среди которых:

– граждане, достигшие возраста привлечения к административной ответственности;

– должностные лица в структуре средств массовой информации, ответственные за выпуск в эфир соответствующей информационной продукции;

– юридические лица.

Субъективная сторона административного правонарушения, предусмотренного ст. 13.15 КоАП РФ, характеризуется совершением с умыслом либо по неосторожности.

Обязательным признаком субъективной стороны рассматриваемого состава административного правонарушения является согласно ст. 2.2 КоАП РФ наличие вины, представляющее из себя психическое отношение виновного лица к совершенным им действиям и возможным последствиям.

Таким образом, злоупотребление свободой массовой информации следует признавать сложным и многоаспектным негативным правовым явлением. Совершение административного правонарушения, ответственность за которое установлена в ст. 13.15 КоАП РФ, сводится не только к нарушению информационных прав и свобод других лиц, но и к воздействию на подсознание людей.

При осуществлении производства по делам об административных правонарушениях в сфере информации нельзя не руководствоваться отдельными положениями постановления Пленума Верховного Суда Российской Федерации от 15 июня 2010 г. № 16 «О практике применения судами Закона Российской Федерации „О средствах массовой информации”»[1] (далее – постановление № 16).

[1] Российская газета. 2010. № 132.

Так, согласно п. 28 постановления № 16, при выяснении вопроса, имело ли место в соответствующем случае злоупотребление свободой массовой информации, суду необходимо выяснять не только употребленные в теле- или радиопрограмме или статье выражения (формулировки) и слова, но и заложенный в них контекст, в рамках которого они были использованы (например, стиль или жанр статьи, программы или ее соответствующей части).

Кроме того, необходимо установить:

– каким образом следует воспринимать выраженные мнения, как политические дискуссии либо некий способ привлечения внимания общества к обсуждению общественно значимых вопросов;

– на чем основаны программа, статья или материал и каково отношение представителя редакции СМИ или интервьюера к суждениям, мнениям, утверждениям, высказанным в ходе проведения программ либо опубликования статей и материалов;

– принимать во внимание существующую на тот момент в стране или в отдельном ее регионе общественную и политическую обстановку (в пределах которого была распространена соответствующая информация).

Вместе с тем, оценивая соответствующую информацию в качестве злоупотребления свободой массовой информации, необходимо также обращать внимание на особенности использования сатирического и юмористического жанров, которые, в отличие от других литературных жанров, в основе построения своих текстов используют больше преувеличения, свободы и гиперболизирования. В то же время граждане не должны вводиться средствами массовой информации в заблуждение относительно этих событий, обстоятельств и фактов.

В целом анализ состава административного правонарушения, предусмотренного ст. 13.15 КоАП РФ, дает возможность прийти к выводу о сложности привлечения к административной

ответственности виновных лиц за совершение подобных противоправных действий, в особенности при совершении данных правонарушений в глобальной сети «Интернет». В каждом случае совершения административного правонарушения необходимо применять индивидуальный подход для выявления соответствующего злоупотребления со стороны средств массовой информации.

Необходимо отметить, что ст. 13.15 КоАП РФ направлена в первую очередь на реализацию требований законодательства о средствах массовой информации и Федерального закона от 25 июня 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»[1] (далее – Федеральный закон «О противодействии экстремисткой деятельности»).

Правонарушения экстремистского характера обладают своеобразной правовой природой. Так, подобные правонарушения совершаются при исторически сложившихся социальных условиях, которые способствуют совершению правонарушений по мотивам расовой, политической, идеологической, национальной или религиозной ненависти, принадлежности к какой-либо социальной группе.

Вместе с тем данные правонарушения направлены против основ конституционного строя, государственной безопасности и целостности конституционных прав и свобод человека и гражданина.

Нельзя не сказать о том, что экстремистская деятельность характеризуется большим масштабом влияния на социальные процессы, отсутствием государственных границ, активным международным взаимодействием, организованной иерархичной структурой.

К характерным признакам проявлений экстремизма можно отнести следующие:

---

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_37867/. Режим доступа: по расписанию.

– отрицание инакомыслия и нетерпимость к представителям других взглядов (политических, экономических, религиозных и иных);

– применение насилия не только к активным противникам экстремистской идеологии, но и к любым лицам, которые не разделяют взгляды и убеждения экстремистов;

– отрицание основных положений известных идеологических и религиозных учений;

– преобладание эмоционального воздействия во время провозглашения пропагандистских идей экстремистского характера, давление на чувства и предрассудки людей, отказ от разумного восприятия;

– возведение лидера экстремистского движения в ранг несокрушимого, а его распоряжений – не подлежащих обсуждению.

Все указанные признаки находятся в тесном взаимодействии между собой, дополняют друг друга и имеют неразрывную внутреннюю связь.

С целью противодействия совершению правонарушений экстремистской направленности законодателем целенаправленно была включена ч. 2 ст. 13.15 в КоАП РФ.

Диспозиция данной статьи признает административным правонарушением распространение информации об общественном объединении или иной организации, включенных в опубликованный перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом «О противодействии экстремистской деятельности», без указания на то, что соответствующее общественное объединение или иная организация ликвидированы или их деятельность запрещена.

Таким образом, можно сделать вывод о том, что деятельность по противодействию экстремизму в административно-правовом аспекте следует рассматривать как урегулированную нормами административного права внешнюю и внутреннюю деятельность уполномоченных государственных органов, направленную на охрану общественного порядка, обеспечение общественной безопасности, жизни и здоровья граждан, конституционного строя государства, государственных границ.

Рассматривая иные составы административных правонарушений, нельзя не сказать о том, что с недавнего времени они включают в себя и нормы, влекущие административную ответственность для публичных органов государственного управления, в том числе для органов местного самоуправления.

Обратим внимание на то, что повышение уровня доверия граждан к органам публичной власти является целью мероприятий по постоянному совершенствованию механизма государственного управления, которое невозможно без привлечения к административной ответственности соответствующих лиц при наличии неоспоримых доказательств совершения правонарушений.

В числе последних тенденций во взаимодействии государственных органов с гражданами явно прослеживается линия все большего применения электронных способов общения с населением.

Так, государственные органы осваивают новые платформы взаимодействия с обществом, модернизируют существующие способы коммуникации с гражданами. Очевидно, что общение органов публичной власти и населения все больше «виртуализируется», переносится в интернет-среду.

По этой причине размещение информации на интернет-ресурсах со стороны органов государственной власти нуждается в нормативном правовом регулировании.

В данном свете особое внимание следует уделить презумпции открытости информации. Если доступ к информации не

ограничен законодательством, такая информация должна быть открытой и при возникающей у граждан необходимости им доступна. В противном случае следует наступление административной ответственности.

Так, в КоАП РФ предусмотрены следующие составы административных правонарушений:

– статья 13.27 «Нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещения в сети «Интернет»;

– статья 13.28 «Нарушение порядка предоставления информации о деятельности государственных органов и органов местного самоуправления».

Последняя статья предусматривает административную ответственность за нарушение порядка предоставления информации, содержащей сведения ограниченного доступа (ч. 1), и за незаконное взимание платы за предоставление информации либо за нарушение порядка взимания платы за предоставление, если такая плата установлена федеральным законом (ч. 2).

Далее перейдем к рассмотрению административно-правовых норм, устанавливающих ответственность за разглашение информации ограниченного доступа.

В ст. 13.14 КоАП РФ закрепляется ответственность за разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей. Меры административно-правовой ответственности, закрепленные в ст. 13.14 КоАП РФ, направлены на охрану и защиту административных правоотношений в сфере информационных технологий, в которых используется информация ограниченного доступа и конфиденциального характера.

Объектом административного правонарушения, предусмотренного ст. 13.14 КоАП РФ, является информация, доступ к которой ограничен федеральным законом. Данное посягательство может быть осуществлено в отношении широкого перечня информации (сведений), имеющих ограничение в обороте, например государственная тайна или сведения инсайдерского характера, и составляющих состав одного административного правонарушения.

Предметом рассматриваемого административного правонарушения следует признать содержание различного рода файлов, документов, баз данных, сведения в которых не являются общедоступными для неопределенного круга лиц, а открыты лишь тому лицу, которое владеет ими на праве собственности или ином праве (доверитель), и лицу, которому данная информация выдана для надлежащего выполнения своих служебных, трудовых и профессиональных обязанностей (конфиденту).

Объективная сторона правонарушения, предусмотренного ст. 13.14 КоАП РФ, состоит в совершении виновным лицом активных действий, направленных на разглашение информации ограниченного доступа. При этом определение термина «разглашение» в действующем административном и уголовном законодательстве отсутствует. В свою очередь, в лингвистическом понимании рассматриваемого термина заложены два способа осуществления подобного действия: устное сообщение сведений или их иное распространение, обращенное неопределенному кругу лиц.

Административное правонарушение, ответственность за которое предусмотрена ст. 13.14 КоАП РФ, совершается специальным субъектом, т. е. лицом, которое получило доступ к сведениям, ограниченным в обороте, в результате осуществления им профессиональных или служебных обязанностей. Следует отметить, что наиболее распространенным субъектом рассматривае-

мого административного правонарушения выступают должностные лица различных органов власти, а также лица, осуществляющие профессиональную деятельность – нотариусы, адвокаты.

С субъективной стороны незаконная деятельность по разглашению информации с ограниченным доступом осуществляется либо с умыслом, либо с неосторожностью.

В целом проведенный анализ состава административного правонарушения, предусмотренного ст. 13.14 КоАП РФ, позволяет сделать вывод о том, что рассматриваемая норма является универсальной, поскольку представляет собой эффективное сдерживающее средство на пути деятельности лиц, распространяющих информацию конфиденциального характера.

Статья 13.14 КоАП РФ отчасти сопряжена со ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных», поскольку персональные данные также относятся к информации, обладающей особым правовым статусом.

Объектом правонарушения рассматриваемой статьи являются общественные отношения, связанные с интересами отдельной личности в информационной сфере, с персональными данными.

Непосредственный объект правонарушения образует право на персональные данные, которое имеет комплексную природу и формируется на основе множества международных, федеральных и локальных нормативных правовых актов.

Так, в ст. 24 Конституции Российской Федерации гражданам гарантируется право на неприкосновенность частной жизни, личную и семейную тайну, ограничивается сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

Значительный перечень международных соглашений, к которым присоединена Российская Федерация и которые ратифицированы на ее территории, также направлены на защиту таких

объектов, как права и свободы человека и гражданина при обработке его персональных данных.

Российское законодательство о персональных данных, представленное в первую очередь Федеральным законом «О персональных данных», постепенно гармонизируется с европейским законодательством. При этом существовавшая ранее плотная связь с информационным и трудовым законодательством постепенно формируется по европейскому образцу.

Отметим, что с целью защиты прав граждан в данной сфере разрабатывается значительный объем подзаконных нормативных правовых актов, например, постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Тем не менее основной массив норм должен быть разработан оператором персональных данных. При обработке персональных данных в системах устанавливаются четыре уровня защищенности в зависимости от категории данных и количества субъектов, данные которых содержит система.

Объективная сторона данного правонарушения представляет собой нарушение порядка обработки персональных данных и включает в себя все деяния в форме действия либо бездействия, установленные федеральным законодательством, ведомственными и локальными нормами, которые не соответствуют правилам (регламенту) обращения с персональными данными.

Субъектами данного правонарушения могут быть как граждане в возрасте от 16 лет, так и должностные лица, в круг должностных обязанностей которых входит решение вопросов по осуществлению деятельности по защите информации о гражданах (персональных данных), а также юридические лица, которые осуществляют деятельность с нарушениями, предусмотренными ст. 13.11 КоАП РФ.

Субъективная сторона административного правонарушения по ст. 13.11 КоАП РФ может иметь место только в форме умысла.

Далее рассмотрим подробно не менее значимую ст. 13.12 КоАП РФ «Нарушение правил защиты информации».

Данная статья предполагает наступление административной ответственности в случаях:

– нарушения условий лицензии на осуществление деятельности в области защиты информации, не отнесенной к государственной тайне;

– использования несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации (за исключением средств защиты информации, составляющих государственную тайну);

– нарушения условий лицензий на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты государственной тайны, осуществлением услуг по защите информации, составляющей государственную тайну;

– использования несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну;

– грубого нарушения условий лицензии на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну).

Ключевым моментом во всех перечисленных случаях является оценка того, относится ли информация, правовой режим которой нарушен, к категории, составляющей государственную тайну.

В соответствии с Законом Российской Федерации «О государственной тайне» под государственной тайной следует понимать защищаемые государством сведения в области его военной,

внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Таким образом, административное расследование и рассмотрение каждого из данных правонарушений требуют профессионального подхода со стороны должностных лиц и наличия специальных знаний, которые бы позволили на должном уровне установить механизм совершения правонарушения и с неоспоримой точностью выявить лицо, виновное в нем.

В заключение хочется еще раз подчеркнуть, что административные правонарушения в области оборота связи и информации объединены в гл. 13 КоАП РФ.

Данные правонарушения по объектному составу условно можно подразделить на несколько групп.

Наиболее обширная группа образована составами правонарушений в области связи. К ним относятся: самовольное подключение к сети электрической связи оконечного оборудования (ст. 13.2 КоАП РФ); нарушение правил охраны линий или сооружений связи (ст. 13.5 КоАП РФ); использование несертифицированных средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия указанным требованиям (ст. 13.6 КоАП РФ); несоблюдение установленных правил и норм, регулирующих порядок проектирования, строительства и эксплуатации сетей и сооружений связи (ст. 13.7 КоАП РФ); самовольные строительство или эксплуатация сооружений связи (ст. 13.9 КоАП РФ).

К данной группе относятся также составы правонарушений, предусмотренные ст. 13.3 «Изготовление или установка радиоэлектронных средств и (или) высокочастотных устройств без специального разрешения (лицензии)» и ст. 13.4 «Нарушение требований к использованию радиочастотного спектра, правил

радиообмена или использования радиочастот, несоблюдение норм или параметров радиоизлучения».

Следующую группу образуют правонарушения, посягающие на установленный законом порядок сбора, хранения, использования, распространения или защиты информации ограниченного доступа. К этой же группе относятся правонарушения, связанные с незаконной деятельностью в области защиты информации (ст. 13.13 КоАП РФ) и разглашением информации с ограниченным доступом (ст. 13.14 КоАП РФ).

Третья группа составов административных правонарушений – это противозаконные деяния в области свободы массовой информации. К ним относятся: злоупотребление свободой массовой информации (ст. 13.15 КоАП РФ); воспрепятствование распространению продукции средства массовой информации (ст. 13.16 КоАП РФ); нарушение правил распространения обязательных сообщений (ст. 13.17 КоАП РФ); воспрепятствование уверенному приему радио- и телепрограмм (ст. 13.18 КоАП РФ).

Действующее административное законодательство в сфере информационных технологий во многом способствует своевременному выявлению и пресечению подобных правонарушений при условии обеспечения надлежащей деятельности соответствующих государственных органов и должностных лиц. Вместе с тем необходимо иметь в виду, что действующий механизм реализации административных правонарушений в сфере информации нуждается в некотором совершенствовании, что позволило бы своевременно и адекватно реагировать на вновь появляющиеся угрозы информационной безопасности.

При этом определенный акцент следует сделать на том, что развитие административного законодательства и, как следствие, порядок признания определенных деяний административно наказуемыми не всегда соответствует темпу развития правонарушений в информационном пространстве.

Так, в мировой действительности распространенность получил вид противоправных деяний, именуемых «фишингом». Сущность данного противоправного деяния заключена в получении доступа к конфиденциальным данным пользователей, логинам и паролям, при помощи сети «Интернет». Целью данного деяния является хищение денежных средств, что влечет уголовную ответственность. Однако в случаях, когда ущерб от данных действий в материальном эквиваленте составляет менее одной тыс. руб. подобные действия вполне обоснованно должны охватываться рамками административной ответственности, но в КоАП РФ к настоящему моменту какая-либо ответственность отсутствует.

Таким образом, институт административной ответственности за правонарушения в сфере информационных технологий находится в динамичном развитии. Действующие нормы КоАП РФ устанавливают ответственность за ряд деяний в сфере киберсреды. Однако реалии современности не позволяют считать сложившуюся административно-правовую систему предупреждения правонарушений в сфере информационного пространства удовлетворительной с учетом постоянного совершенствования кибернетических угроз. Отметим, что по этой причине административное законодательство в данный момент подвержено ряду реформ, которые найдут отражение в будущем кодифицированном административно-деликтном законодательстве Российской Федерации.

ГЛАВА 3. Актуальные проблемы квалификации преступлений в сфере информационных технологий

§ 3.1. Уголовно-правовая характеристика преступлений в сфере компьютерной информации (гл. 28 УК РФ)

Значительное количество хищений, совершаемых в системах дистанционного банковского обслуживания (далее – ДБО), сопряжено с предварительным посягательством на отношения, обеспечивающие безопасность соответствующих информационных ресурсов. В российском уголовном законодательстве данные деяния именуются как преступления в сфере компьютерной информации и определены в гл. 28 УК РФ. Вопросы их практического применения достаточно активно разрабатываются в отечественной науке. Однако следует констатировать, что многие аспекты квалификации соответствующих посягательств до настоящего времени имеют неразрешенный характер.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)

Рис. 3.1. Количество зарегистрированных преступлений по ст. 272 УК РФ

Объектом данного преступления выступают общественные отношения, связанные с обеспечением конфиденциальности, целостности и (или) доступности охраняемой законом компьютерной информации.

Следует отметить, что в российской науке до настоящего времени нет общепринятого подхода относительно толкования «охраняемой законом информации». Достаточно распространенной стала позиция ограничительного толкования данного признака, при котором под такой информацией предлагается понимать лишь конфиденциальную информацию[1].

В судебной практике можно обнаружить примеры применения ст. 272 УК РФ и в тех случаях, когда лицо совершило модификацию либо уничтожение открытой информации. Так, С., уволившись из организации, испытывая неприязненное отношение к руководству, желая опорочить деловую репутацию хозяйствующего субъекта, уничтожил и модифицировал часть компьютерной информации: изменил изображение слайдера, удалив исходные изображения, но добавив другие изображения, порочащие деловую репутацию Общества, удалил контактный телефон и сведения об имеющихся сертификатах, изменил сведения о производстве и качестве сырья, удалил информацию о партнерах, экологической безопасности продукции и т. д.[2]

Подобная практика основывается на положениях Федерального закона «Об информации, информационных технологиях и о защите информации». Согласно ст. 16 данного закона защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/-prime/doc/70542118/.

[2] Приговор Октябрьского районного суда г. Архангельска от 14 декабря 2015 г. по делу № 1-352/2015 // Судебные и нормативные акты РФ. URL: https://sudact.ru/.

информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

Такой подход расширительного толкования предмета преступления, предусмотренного ст. 272 УК РФ имеет место быть. Достаточно сложно привести аргументы в пользу того, почему в эпоху информационного общества из трех значимых качеств компьютерной информации, уголовно-правовой охраной может быть обеспечено лишь одно. Общедоступная информация не лишена защиты. Положения об обязательном характере технологической и программной защиты общедоступной информации, размещаемой в сети «Интернет», содержатся во многих подзаконных нормативных правовых актах. Таким образом, по смыслу ст. 272 УК РФ к охраняемой законом информации следует относить не только информацию ограниченного доступа, но и общедоступную информацию, в отношении которой ее обладателем приняты меры по защите от несанкционированного уничтожения, модификации или блокирования.

Объективная сторона преступления выражается в неправомерном (противоречащем закону или иному нормативному акту) доступе к компьютерной информации.

По конструкции объективной стороны состав является материальным и считается оконченным с момента наступления хотя бы одного из альтернативных последствий: уничтожения, блокирования, модификации либо копирования компьютерной информации. Данные признаки хорошо раскрыты в отечественной теории уголовного права и, как показывает изучение правоприменительной практики, не вызывают значительных затруднений у правоприменителей. Отдельно следует указать, что само по себе наличие архивных копий тех или иных данных у правообладателя не препятствует уголовному преследованию по ст. 272 УК РФ. Кроме того, значимым аспектом познания анализируемого состава является

то, что в нем зачастую момент юридического и фактического окончания не совпадают. Так, лицо, получив неправомерный доступ к чужому аккаунту, де-факто совершило уже оконченный состав преступления, предусмотренный ст. 272 УК РФ. Вместе с тем фактическое окончание данного преступления может быть значительно отдален от данного момента и связан с различными обстоятельствами объективной действительности. Это в обязательном порядке необходимо учитывать при исчислении сроков давности привлечения к ответственности по соответствующей категории дел.

Субъект основного состава общий, т. е. физическое, вменяемое лицо, достигшее шестнадцатилетнего возраста.

Несмотря на то, что диспозиция рассматриваемой статьи не дает прямых указаний относительно субъективной стороны преступления, можно с уверенностью говорить об умышленной форме вины в виде прямого или косвенного умысла. Крайне дискуссионной является позиция, встречающаяся в отечественной литературе, что субъективная сторона данного преступления характеризуется альтернативно также и неосторожностью. Уязвимость этого толкования проявляется как в нарушении системного подхода к толкованию компьютерных преступлений в целом, так и в неправильном понимании специфики самой объективной стороны неправомерного доступа к соответствующим данным. Доступ здесь во многом синонимичен с таким термином, как проникновение, которое по определению предполагает известную целенаправленность действия. Следовательно, не может быть ответственности в рамках ст. 272 УК РФ за совершение неосторожных действий, в результате которых были уничтожены компьютерные данные.

К квалифицирующим признакам, названным в ч. 2 ст. 272 УК РФ, относится совершение данного преступления с причинением крупного ущерба (свыше одного млн руб. или из корыст-

ной заинтересованности. Корыстная заинтересованность при совершении данного преступления выражается в стремлении лица извлечь материальную выгоду из преступления для себя лично или других лиц.

Часть 3 ст. 272 УК РФ предусматривает три особо квалифицирующих признака. Неправомерный доступ к охраняемой законом компьютерной информации, совершенный: 1) группой лиц по предварительному сговору; 2) организованной группой; 3) лицом с использованием своего служебного положения. Понимание данных видов квалифицированного неправомерного доступа к компьютерной информации в целом основывается на обращении к положениям ст. 35 УК РФ. Следует лишь указать, что совершение данного преступления в соучастии довольно часто не предполагает непосредственного (реального) взаимодействия субъектов, которые преимущественно коммуницируют в виртуальном мире. Однако это не оказывает значимого влияния на юридическую оценку имевшего место соучастия.

Часть 4 ст. 272 УК РФ предусматривает два особо квалифицирующих признака. Неправомерный доступ к охраняемой законом компьютерной информации, если такие действия повлекли тяжкие последствия или создали угрозу их наступления.

Следует специально отметить, что данный особо квалифицированный вид неправомерного доступа к компьютерной информации в наибольшей степени конкурирует с положениями ст. 274.1 УК РФ «Неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации». Здесь отечественная теория уголовного права еще не выработала общих и четких критериев отграничения составов.

Рис. 3.2. Количество зарегистрированных преступлений по ст. 273 УК РФ

Объектом преступления выступают общественные отношения, связанные с обеспечением информационной безопасности от негативного воздействия вредоносной компьютерной информации и вредоносных компьютерных программ.

Содержание предмета данного преступления, а именно вредоносной компьютерной информации и вредоносной компьютерной программы, в целом выводится из грамматического, логического и формально-юридического анализа диспозиции ст. 273 УК РФ.

На правоприменительном уровне наиболее часто совершение данного преступления фиксируется при использовании и распространении вредоносных компьютерных программ, которые заведомо предназначены для генерации кода установки (серийного номера) и кода активации, запрашиваемых при установке лицензионных программных продуктов.

Следует отметить, что установление предмета данного преступления предполагает проведение соответствующих экспертиз,

которые сам признак вредоносности не устанавливают, однако позволяют предельно четко представить функциональные особенности компьютерной информации или программы. Вывод о вредоносности лежит уже в плоскости юридической квалификации на основании заключения эксперта.

С объективной стороны преступление проявляется в совершении хотя бы одного из следующих действий:

– создание компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

– использование таких компьютерных программ или такой компьютерной информации;

– распространение таких компьютерных программ или такой компьютерной информации.

Следует обратить внимание на то, что создание, использование и распространение вредоносных компьютерных программ или вредоносной компьютерной информации, всегда предполагает активные действия со стороны лица, совершившего это преступление. Бездействием совершить рассматриваемое преступление не представляется возможным.

Следует согласиться с мнением, что использование вредоносной компьютерной программы для личных нужд (например, для уничтожения собственной компьютерной информации) ненаказуемо[1]. Таким образом, в тех случаях, когда вредоносная программа не создает угрозы для безопасности компьютерной информации, действия лица правомерно расценивать как малозначительные (ч. 2 ст. 14 УК РФ).

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/-prime/doc/70542118/.

Указанное частное правило квалификации распространяется и на те ситуации, когда соответствующие манипуляции с вредоносными компьютерными объектами совершают работники сферы информационной безопасности для тестирования соответствующих систем и программно-технических комплексов.

Состав преступления, предусмотренный ч. 1 ст. 273 УК РФ, сконструирован по типу формального.

Если создание, использование или распространение вредоносных программ выступает в качестве способа совершения иного умышленного преступления, то содеянное надлежит квалифицировать по совокупности преступлений. Например, в тех случаях, когда вредоносная программа создается или используется с целью устранения установленных правообладателем средств индивидуальной защиты компьютерной программы, ответственность наступает по соответствующим частям ст.ст. 146 и 273 УК РФ.

Субъектом создания, использования и распространения вредоносных компьютерных программ может являться любое физическое вменяемое лицо, достигшее шестнадцатилетнего возраста.

С субъективной стороны данное преступление совершается только с прямым умыслом. Мотивы анализируемого преступления и его цели не являются обязательными признаками состава и учитываются лишь при назначении наказания.

В том случае, если виновный при использовании или распространении вредоносных программ умышленно уничтожил или повредил технику, что причинило значительный ущерб потерпевшему, то его поведение образует совокупность преступлений, предусмотренных ст.ст. 167 и 273 УК РФ.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей (ст. 274 УК РФ)

Рис. 3.3. Количество зарегистрированных преступлений по ст. 274 УК РФ

Объектом рассматриваемого преступления является совокупность общественных отношений в сфере соблюдения установленных 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.

Диспозиция ст. 274 УК РФ бланкетная. Поэтому для уяснения признаков объективной стороны преступления необходимо прежде всего обратиться к тем конкретным положениям, закрепляющим правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правила доступа к информационно-телекоммуникационным сетям, которые были нарушены виновным.

В отличие от ряда иных специальных правил, сосредоточенных в конкретных нормативных актах, правила эксплуатации средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей не консолидированы и содержатся во множестве источников.

Бытовая небрежность, повлекшая уничтожение или повреждение компьютерного оборудования, уничтожение или модификацию данных и, как следствие, причинение имущественного ущерба потерпевшему не может быть квалифицировано по ст. 274 УК РФ. При подобных обстоятельствах содеянное не образует признаков какого-либо преступления и может выступать основанием для дисциплинарной и гражданско-правовой ответственности работника.

Объективная сторона преступного нарушения 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 состоит из общественно опасного деяния в форме действия или бездействия, наступивших общественно опасных последствий и причинной связи между ними.

Обязательным признаком объективной стороны этого преступления являются общественно опасные последствия. При этом необходимо отметить, что закон в ст. 274 УК РФ выделяет как бы два уровня последствий, каждый из которых является обязательным для признания состава преступления оконченным. В качестве последствий основного состава преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования является уничтожение, блокирование, модификация либо копирование охраняемой законом компьютерной информации и причинение крупного ущерба (в соответствии с примечанием к ст. 272 УК РФ ущерб, сумма которого превышает один млн руб.).

Таким образом, формулировка закона исключает возможность привлечения лица к уголовной ответственности по ст. 274 УК РФ, если нарушение указанных правил хотя и повлекло уничтожение, блокирование, модификацию либо копирование информации, но объективно не причинило крупного ущерба.

Субъектом преступления, предусмотренного ст. 274 УК РФ, является физическое, вменяемое лицо, достигшее к моменту совершения преступления шестнадцатилетнего возраста, на которое в силу закона, иного нормативного акта либо характера выполняемой профессиональной, трудовой или иной деятельности возложена обязанность по соблюдению соответствующих правил эксплуатации или доступа.

В теории уголовного права обосновывается позиция, согласно которой субъектом преступного деяния, предусмотренного ст. 274 УК РФ, будет являться любое физическое, вменяемое лицо, достигшее к моменту совершения преступления шестнадцатилетнего возраста, т. е. общий субъект преступления. Такой подход является дискуссионным и не позволяет провести четкое отграничение исследуемого преступного деяния от неправомерного доступа к компьютерной информации. Как совершенно справедливо резюмирует по данному поводу Р. Р. Гайфутдинов, по смыслу ст. 274 УК РФ у лица имеется доступ к соответствующим объектам информационно-коммуникационной инфраструктуры[1]. Имеется в виду правомерный доступ. Специализация субъекта здесь может определяться не только тем, что на лицо конкретными инструкциями или договорами возложены обязанности по соблюдению соответствующих правил, но и самим фактом использования лицом соответствующих ресурсов и (или) оборудования, т. е. определяться фактической включенностью лица в специфическую группу общественных отношений. Присоединение к любому пользовательскому соглашению,

[1] Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации : дис. … канд. юрид. наук. Казань, 2017. С. 142.

которое, как известно, осуществляется лицом путем проставления соответствующей отметки при прохождении регистрации на том или ином ресурсе, автоматически включает его в такие отношения.

Здесь нужно прибегнуть к историческому толкованию действующей редакции ст. 274 УК РФ. Как известно, до внесения изменений Федеральным законом от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» диспозиция анализируемой нормы содержала оговорку о том, что нарушение правил эксплуатации должно быть допущено лицом, «имеющим доступ к ЭВМ, системе ЭВМ или их сети». Справедливо отказываясь от архаизмов в тексте закона в пользу более универсальной категории средства хранения, обработки или передачи компьютерной информации, законодатель по какой-то причине (изучение паспорта законопроекта[1] ответа на этот вопрос не дает) исключает специальное указание на признаки специального субъекта в тексте нормы. Предполагается, что действующая редакция могла показаться законодателю в некотором смысле «перегруженной», тавтологичной – нарушение правил эксплуатации предполагает, что лицо было к такой эксплуатации допущено. Однако верифицировать это предположение не представляется возможным.

Исключение специального указания о наличии у субъекта преступления, предусмотренного ст. 274 УК РФ, правомочий по доступу к соответствующим средствам хранения, обработки или передачи компьютерной информации, и без того усложнило понимание содержания данной уголовно-правовой нормы. Прежде всего это нашло свое проявление в отграничении нарушения

[1] Паспорт проекта федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (в части совершенствования законодательства Российской Федерации)» // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/.

правил эксплуатации от неправомерного доступа к компьютерной информации, совершенного лицом с использованием своего служебного положения (ч. 3 ст. 272 УК РФ).

В правоприменительной практике сложился подход, согласно которому неправомерность доступа к компьютерной информации определяется не только полномочиями субъекта по самому доступу, но и правомочиями по копированию, модификации, блокированию или уничтожению информации. Такое расширительное толкование неправомерного доступа к компьютерной информации не может не приводить к путанице в понимании как самого неправомерного доступа к компьютерной информации, так и нарушения правил эксплуатации средств ее хранения, обработки или передачи. В качестве примера можно привести следующее судебное решение.

Занимая должность менеджера по продажам дополнительного офиса банка, В., желая иметь статус эффективного работника, с целью исполнения возложенных на нее обязанностей по выполнению индивидуального плана, в нарушение Инструкции Центробанка Российской Федерации… а также внутренних нормативных и распорядительных документов, реализуя единый преступный умысел на неправомерный доступ к охраняемой законом компьютерной информации, используя возможность доступа к охраняемой законом компьютерной информации, в связи с исполнением должностных обязанностей и выполняемой работы, посредством служебного компьютера, осознавая, что не сможет исполнить возложенные на нее обязанности по выполнению индивидуального плана… неправомерно вошла в программу ФП «Банковские карты», которая обеспечивает доступ к центральной базе данных филиала, используя свои логин и пароль, предоставленные ей в силу служебных полномочий, тем самым преодолев средства защиты, в отсутствии реального обращения клиентов, выполнила операции по выдаче банковской карты категории Momentum на имя указанных лиц. Далее была

произведена активизация выпущенных карт и счетов на имя указанных лиц, что повлекло за собой модификацию компьютерной информации, с использованием своего служебного положения, в связи с чем были похищены денежные средства у указанных лиц и наступившие последствия причинили вред деловой репутации банка.

В приговоре суд указывает на обстоятельства, которые вступают уже в прямое противоречие с самой квалификацией деяния по ст. 272 УК РФ: «…При этом доступ к центральной базе данных филиала В. был предоставлен работодателем при трудоустройстве последней, путем присвоения ей логина, создания пароля и предоставления электронной цифровой подписи, находящейся на ТМ-идентификаторе, которые В. использовала при исполнении ею своих служебных обязанностей, в связи с чем в судебном заседании установлено наличие в действиях В. квалифицирующего признака с использованием своего служебного положения, предусмотренного ч. 3 ст. 272 УК РФ, ввиду того, что она при совершении инкриминируемых деяний, связанных с модификацией охраняемой законом компьютерной информации, содержащейся в центральной базе данных филиала, имела к ней доступ в силу исполнения ею своих должностных обязанностей»[1].

Как представляется, работник кредитной организации, обладая неаннулированным доступом к служебной базе данных, имея соответствующие сетевые идентификаторы для работы, не может совершить неправомерный доступ к хранящейся в ней информации. Вместе с тем такой работник может нарушить правила эксплуатации такой системы, как в приведенном решении – внести недостоверные сведения об обращениях клиентов банка за выдачей платежных карт.

---

[1] Приговор Ленинского районного суда г. Курска от 8 августа 2019 г. № 1-336/4-2019 // Судебные и нормативные акты РФ. URL: https://sudact.ru/.

Практика квалификации действий, связанных с уничтожением, модификацией или копированием охраняемой законом компьютерной информации, совершенных лицами, которые на законных основаниях используют компьютерную информацию и средства ее обращения (программисты, системные администраторы, администраторы баз данных, специалисты по эксплуатации объектов информационно-телекоммуникационной инфраструктуры и др.), как неправомерного доступа по ч. 3 ст. 272 УК РФ является широко распространенной[1]. Объективная необходимость каким-либо образом реагировать на подобные инциденты служебного злоупотребления со стороны лиц, которым были доверены соответствующие объекты информационно-телекоммуникационной инфраструктуры, вместе с трудностями в установлении требуемого ст. 274 УК РФ крупного ущерба обусловили искусственное расширение пределов действия уголовно-правового запрета об ответственности за неправомерный доступ.

Субъективная сторона преступного нарушения 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 характеризуется двумя формами вины. Нарушение правил эксплуатации и доступа, предусмотренное ч. 1 ст. 274 УК РФ, может совершаться как умышленно (при этом умысел должен быть направлен на нарушение правил эксплуатации и доступа), так и по неосторожности.

[1] Русскевич Е. А. О квалификации преступлений в сфере компьютерной информации, совершаемых с использованием служебного положения // Российское правосудие. 2019. № 2. С. 35–41.

Неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274.1 УК РФ)

Информационная безопасность уже на протяжении длительного времени входит в актуальную повестку государственной политики России. Об этом регулярно высказываются первые лица страны, принимаются законы и подзаконные нормативные правовые акты, цифровизация обсуждается на крупных дискуссионных площадках и научных форумах, в рамках целевых национальных программ выделяются значительные средства для создания устойчивой и безопасной информационно-коммуникационной инфраструктуры.

В период пандемии COVID-19, когда предпринятые государством меры социальной изоляции вовлекли в орбиту цифровых технологий новых пользователей, вынужденных работать удаленно, обеспечение информационной безопасности приобрело еще более актуальный характер.

Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и ст. 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона „О безопасности критической информационной инфраструктуры Российской Федерации”»[1] дополнил гл. 28 УК РФ специальной нормой об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274.1).

В 2018 г. было зарегистрировано лишь одно преступление, предусмотренное ст. 274.1 УК РФ (в Камчатском крае), в 2019 г. – 4 (Амурская область – 1, Волгоградская область – 1, Приморский край – 2), а в 2020 г. было зарегистрировано уже 22 преступления (Амурская область – 1, Волгоградская область – 9, Ивановская

[1] Российская газета. 2017. № 167. 31 июля.

область – 1, Кемеровская область – 1, Москва – 1, Мурманская область – 1, Пермский край – 1, Приморский край – 3, Республика Северная Осетия-Алания – 1, Республика Татарстан – 1, Республика Хакасия – 1, Тверская область – 1)[1].

Объектом преступлений, предусмотренных ст. 274.1 УК РФ, выступает безопасность критической информационной инфраструктуры Российской Федерации, т. е. состояние ее защищенности от любого воздействия программными или программно-техническими средствами, которое способно привести к нарушению ее функционирования и (или) нарушению безопасности обрабатываемой информации.

Предметом преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, является компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры.

Специфическим предметом преступлений, предусмотренных чч. 2 и 3 ст. 274.1 УК РФ, выступают объекты критической информационной инфраструктуры: информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности.

По признаку предмета преступления анализируемая уголовно-правовая норма конкурирует сразу с тремя статьями (ст.ст. 272–274 УК РФ) и является специальной по отношению к ним.

---

[1] По данным ГИАЦ МВД России.

Относимость того или иного информационного ресурса к критическому определяется посредством его включения в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»).

Объективная сторона преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, предполагает совершение любого из трех альтернативных действий:

– создание;

– использование;

– распространение компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры.

Состав по конструкции (по моменту описания в законе момента окончания преступления) является формальным. Если лицо одновременно разработало, использовало и распространило вредоносную компьютерную программу, заведомо предназначенную для совершения компьютерных атак на объекты критической информационной инфраструктуры, содеянное образует единое преступление.

Объективная сторона преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре. Состав по конструкции является материальным. Преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. Таким образом, сам по себе неправомерный доступ по смыслу ч. 2 ст. 274.1 УК РФ не является преступлением.

Вред как конструктивный признак состава преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, не конкретизирован. Системное толкование отечественного уголовного законодатель-

ства позволяет сделать вывод, что таковым является уничтожение, блокирование, модификация, копирование информации, содержащейся в критической информационной инфраструктуре, нейтрализация средств защиты указанной информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование критической информационной инфраструктуры.

В качестве примера можно привести приговор Первомайского районного суда г. Владивостока. О., Л.А и Л.С. были осуждены по ч. 4 ст. 274.1 УК РФ. О., действуя по предварительному сговору с Л.А. и Л.С., используя вредоносную компьютерную программу в нарушение ч. 4 ст. 29 Конституции Российской Федерации, чч. 1, ч. 2 и п. 3 ч. 3 ст. 5, пп. 1–3 ч. 1 ст. 16 и ст. 17 Федерального закона «Об информации, информационных технологиях и о защите информации», с целью выявления уязвимых машин (персональных компьютеров различных организаций) осуществил нейтрализацию средств защиты компьютерной информации путем перебора логина и пароля и произвел сканирование диапазона IP-адресов Российской Федерации в целях выявления открытых портов и дальнейшей проверки их на наличие возможности удаленного к ним доступа по RDP-протоколу. В свою очередь, Л.А. и Л.С., действуя совместно, согласно достигнутой ранее преступной договоренности, используя предоставленную О. информацию о выявленных IP-адресах, номерах портов подключения, логинах и паролях доступа к ЭВМ, при помощи компьютерной программы получили удаленный доступ к ЭВМ АО «Восточная верфь», после чего осуществили неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации путем ее блокирования и модификации, что повлекло причинение вреда критической информационной инфраструктуре АО «Восточная верфь», и причинение имущественного вреда указанной организации на сумму 655 034,52 руб.

Таким образом, Л.А., Л.С. и О., действуя совместно и по предварительному сговору, осуществили модификацию и блокирование охраняемой компьютерной информации, содержащейся в информационных системах и информационно-телекоммуникационных сетях, функционирующих в субъекте оборонной промышленности АО «Восточная верфь», что повлекло причинение вреда критической информационной инфраструктуре, выразившегося в модификации компьютерной информации и воздействиях на компьютерную информацию и технику, последствием которого невозможно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, совершив действия, приводящие к ограничению и закрытию доступа к компьютерному оборудованию и находящейся на них компьютерной информации[1].

Объективная сторона преступления, предусмотренного ч. 3 ст. 274.1 УК РФ, заключается в нарушении:

– правил эксплуатации: средств хранения, обработки или передачи охраняемой компьютерной информации; информационных систем; информационно-телекоммуникационных сетей; автоматизированных систем управления; сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации;

– правил доступа к указанным средствам, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

Состав по конструкции является материальным, преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации.

---

[1] Приговор Первомайского районного суда г. Владивостока от 25 сентября 2019 г. по делу № 1-376/2019 // Судебные и нормативные акты РФ. URL: https://sudact.ru/.

Совершение компьютерных атак на информационные ресурсы объектов транспорта, оборонной, атомной, ракетно-космической или химической промышленности может содержать признаки и других преступлений, предусмотренных ст.ст. 205, 275, 276, 281 УК РФ и др.

Субъектом преступлений, предусмотренных чч. 1 и 2 ст. 274.1 УК РФ, является физическое вменяемое лицо, достигшее шестнадцатилетнего возраста. Субъектом ч. 3 ст. 274.1 УК РФ может быть как общий – в части правил доступа к ресурсам, так и специальный – в части соблюдения правил эксплуатации соответствующих средств, систем и сетей.

Субъективная сторона создания, использования и распространения компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры, характеризуется прямым умыслом. Лицо, совершая те или иные действия, должно осознавать, что они направлены на публичные информационные ресурсы, обладающие исключительной важностью для общества и государства и включенные в соответствующий реестр.

При неправомерном доступе (ч. 2 ст. 274.1 УК РФ) умысел может быть как прямым, так и косвенным.

Субъективная сторона преступления, предусмотренного ч. 3 ст. 274.1 УК РФ характеризуется двумя формами вины.

Анализируя положения Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» в аспекте ст. 274.1 УК РФ, можно сделать вывод, что законодателю не удалось добиться единства позитивного и охранительного механизмов. В УК РФ не были включены значимые правила, нарушение которых объективно представляет опасность не только для для критической информационной инфраструктуры Российской Федерации, но и для иных охраняемых уголовным законом интересов (жизни, здоровья, собственности и т. д.).

В ряду таковых особо следовало бы выделить обязанности соответствующих субъектов, заключающиеся:

1) в незамедлительном информировании о компьютерных инцидентах федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

2) оказании содействия должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) обеспечении выполнения порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

4) реагировании на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

5) обеспечении беспрепятственного доступа должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, к значимым объектам критической информационной инфраструктуры при реализации этими лицами полномочий, предусмотренных законом.

Указанные положения закона в целом направлены на достижение транспарентности и кооперации. Практика сокрытия проблем в сфере информационной безопасности хорошо известна. Специалисты отмечают, что компании неохотно сообщают об инцидентах, связанных с утечкой пользовательской информации. Это влечет за собой репутационные и неизбежные финансовые потери. Те же, кто решается на откровенность, зачастую не спешат с неприятными новостями. Между обнаружением бреши в безопасности и ее обнародованием в некоторых случаях проходят месяцы[1].

Неисполнение указанных выше обязанностей соответствующими субъектами объективно создает угрозу причинения вреда не только состоянию защищенности критической информационной инфраструктуры Российской Федерации, но и правам и свободам отдельных граждан и организаций. Замалчивание компьютерных инцидентов дает фору преступникам, позволяет им осуществлять новые компьютерные атаки.

Принимая во внимание необходимость неукоснительного исполнения субъектами критической информационной инфраструктуры требований регулятивного законодательства в данной сфере, отдельные страны устанавливают уголовную ответственность. Так, Закон о кибербезопасности 2018 г. Сингапура предусматривает значительное количество составов преступлений, связанных с ненадлежащим исполнением правил и стандартов, касающихся функционирования объектов критической информационной инфраструктуры, совершаемых их владельцами/операторами:

1) невыполнение предписания уполномоченного органа, касающегося действий, которые должны быть предприняты владельцем или владельцами в отношении: угрозы кибербезопасности; соблюдения стандартов деятельности, применимых к владельцу;

[1] Сборник исследований по практической безопасности АО «Позитив Текнолоджиз». М., 2018. С. 68.

назначения аудитора, утвержденного уполномоченным органом; других вопросов, которые уполномоченный орган может счесть необходимыми или целесообразными для обеспечения безопасности критически важной информационной инфраструктуры (ст. 12) – наказывается штрафом в размере до 100 тыс. долл. США или лишением свободы на срок до двух лет;

2) несообщение владельцем критически важной информационной инфраструктуры уполномоченному органу о наступлении любого из следующих событий в установленной форме и в установленном порядке в течение установленного периода: инцидент кибербезопасности в отношении критически важной информационной инфраструктуры; инцидент кибербезопасности в отношении любого компьютера или компьютерной системы, находящейся под контролем владельца, которая взаимосвязана или взаимодействует с критически важной информационной инфраструктурой; любой другой тип инцидента кибербезопасности в отношении критически важной информационной инфраструктуры (ст. 14) – наказывается штрафом в размере до 100 тыс. долл. США или лишением свободы на срок до двух лет;

3) уклонение от обязательного аудита состояния защищенности объектов критической информационной инфраструктуры (ст. 15) – наказывается штрафом в размере до 100 тыс. долл. США или лишением свободы на срок до двух лет;

4) уклонение владельца критически важной информационной инфраструктуры от выполнения обязательных требований уполномоченного органа в условиях, требующих обнаружения и предупреждения угроз для национальной безопасности, обороны, международных отношений, экономики, общественного здравоохранения, общественной безопасности или общественного порядка Сингапура (ст. 23) – наказывается лишением свободы на срок до 10 лет[1].

---

[1] URL: https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312.

Данный подход не реализован в отечественном правовом поле. Положения ч. 3 ст. 274.1 УК РФ не распространяются на случаи неисполнения приведенных выше обязанностей, поскольку в целом обращены к эксплуатационным правилам и требованиям средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре.

В отечественной теории уголовного права справедливо подчеркивается, что появление новых технических, военных систем и другие факторы предопределяют дальнейшее расширение сферы действия института ответственности за нарушение специальных обязанностей. Наличие указанного института является необходимым условием реализации субъективных прав и свобод граждан, нормального функционирования общественных отношений в целом, эффективного и безопасного использования различных технических средств[1]. В этом отношении перспективным видится дополнение гл. 28 УК РФ специальной нормой об ответственности за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Однако процесс криминализации требует взвешенного подхода. Так, установление уголовной ответственности за уклонение от исполнения отдельных обязанностей лицами, ответственными за обеспечение безопасности объектов критической информационной инфраструктуры, может быть реализовано двумя способами:

1) путем построения соответствующего состава с административной преюдицией (в этом случае дополнения потребует и отечественный закон об административных правонарушениях);

[1] Уголовная ответственность за преступления, связанные с нарушением специальных правил : монография / [В. К. Андрианов и др.] ; под ред. Ю. Е. Пудовочкина. М. : РГУП, 2018. С. 19.

2) посредством определения состава преступления с материальной конструкцией, включив в качестве криминообразующих признаков причинение крупного ущерба либо наступление тяжких последствий.

Согласимся, что в стремлении избежать декларативности отдельных положений закона о критической информационной инфраструктуре Российской Федерации, обеспечить их эффективным средством правового принуждения необязательно сразу прибегать к очередной модернизации УК РФ. Запретить под страхом ответственности – не значит решить проблему государственно-частного партнерства в сфере обеспечения информационной безопасности. Несомненно одно – затронутая проблема нуждается в обстоятельной проработке и обсуждении профессиональным сообществом.

§ 3.2. Особенности квалификации отдельных видов хищений, совершаемых с использованием информационных технологий

Информационно-коммуникационные технологии стремительно развиваются и все прочнее входят в повседневную жизнь. В современном мире вряд ли осталась хоть одна сфера человеческой деятельности, в которую цифровизация не принесла бы значимых изменений. Мы уже привыкли к тому, что обмениваться личными и деловыми письмами удобнее по электронной почте, приобретать товары комфортнее, а в условиях пандемии COVID-19 и безопаснее, дистанционно через онлайн-магазины. Электронные средства платежа медленно, но уверенно вытесняют их «материальных» соседей. Управление личными финансами (открытие вкладов, оформление кредитов и т. п.) уже не требует непосредственного посещения кредитной организации и без за-

труднений осуществляется через мобильное приложение. Цифровизация изменила наши дома: появилась «умные» бытовые приборы, которые «знают» наши предпочтения, следят за нашей безопасностью, уведомляют о необходимости совершения платежей и т. п.

Сегодня можно с уверенностью утверждать, что Российская Федерация вступила в постиндустриальную фазу развития рыночных отношений, которая включает в себя зарождение и развитие новых институтов, благодаря которым происходит поэтапная интеграция страны в современную «диджитализированную» экономическую систему XXI в.

Реалии убедительно свидетельствуют о том, что по-настоящему развитая экономика все в большей мере базируется на компьютерных технологиях, которые присутствуют практически во всех странах мира, объединяя их в единое «информационное целое».

Наиболее активное развитие в последние годы приобрела цифровизация бумажных денег и носителей информации, которые медленно, но уверенно стали вытеснять их «материальных» соседей. Так, по информации департамента Национальной платежной системы Банка России, по итогам первого полугодия 2020 г. количество безналичных платежей составило почти 69 %, а за год регулятор прогнозирует, что данный показатель превысит 70 %. Россия по этому показателю находится в мировых лидерах. Не стоит на месте и нормативное регулирование данной сферы. Так, в 2011 г. был принят Федеральный закон от 27 июля 2011 г. № 161-ФЗ «О национальной платежной системе»[1].

Недостаточное (во многом фрагментарное) регулирование данной сферы и отсутствие единого толкования законодательных конструкций на уровне правоприменения приводят к многочисленным проблемам при квалификации преступлений по отечественному уголовному закону.

---

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_115625/.

Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[1] была скорректирована диспозиция ст. 159.3 УК РФ, а также дифференцирована ответственность по п. «г» ч. 3 ст. 158 УК РФ.

29 сентября 2020 г. вышло знаковое определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации по делу Ю. Ю. Кактана, во многом изменившее сложившийся подход к разграничению ст. 159.3 и п. «г» ч. 3 ст. 158 УК РФ[2].

До принятия Верховным Судом Российской Федерации указанного решения в судебно-следственной практике хищение безналичных денег с использованием ЭСП оценивалось неоднозначно. Так, по пп. «а, в» ч. 2 ст. 158 УК РФ и ч. 2 ст. 159.3 УК РФ были квалифицированы действия лиц, которые, похитив из салона автомобиля кошелек, впоследствии воспользовались находившейся там банковской картой потерпевшего для оплаты товара в магазине на общую сумму 1 585 руб. 68 коп.

Здесь судебно-следственные органы в целом демонстрируют приверженность той позиции, что, если лицо не изымало соответствующие денежные средства в банкомате, не осуществляло их перевод на другой (подконтрольный ему) банковский счет, а, завладев электронным средством платежа, приобрело товары в магазине, содеянное необходимо квалифицировать по ст. 159.3 УК РФ.

С другой стороны, можно обнаружить значительное количество примеров квалификации похожий ситуаций по п. «г» ч. 3 ст. 158 УК РФ.

---

[1] СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_296451/.

[2] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29 сентября 2020 г. № 12-УДП20-5-К6 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=ARB;n=677229#4Gx17nSiAT0abcPC1. Режим доступа: по расписанию.

В теории, как и на практике, высказывались различные мнения касательно данной проблемы квалификации. Одни специалисты утверждают, что при совершении хищения безналичных денег с использованием ЭСП необходимо применять п. «г» ч. 3 ст. 158 УК РФ, другие склоняются к оценке подобных действий по ст. 159.3 УК РФ.

13 мая 2019 г. Ю. Ю. Кактан нашел банковскую карту. Используя функцию бесконтактной оплаты, Ю. Ю. Кактан приобрел товары в различных магазинах на общую сумму 3 026 руб. 54 коп. Свои действия он не смог довести до конца вследствие того, что банковская карта была заблокирована ее владельцем.

Шестой кассационный суд общей юрисдикции изменил квалификацию действий Ю. Ю. Кактана с ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ на ч. 3 ст. 30, ч. 1 ст. 159.3 УК РФ. Анализ принятого решения позволяет заключить, что суд истолковал содержание «карточного мошенничества» в традиционном его понимании. Поскольку Ю. Ю. Кактан не просто похитил деньги с банковской карты, а использовал ее как средство оплаты товаров в магазинах, его действия выявляют признаки обмана работников этих организаций, которые полагали, что он распоряжается средствами на карте законно.

Верховный Суд Российской Федерации, не согласившись с таким решением, также указал, что для мошенничества с использованием ЭСП обязательным выступает способ совершения преступления – изъятие денег должно быть осуществлено путем обмана или злоупотребления доверием их владельца или иного уполномоченного лица. Вместе с тем в деле Ю. Ю. Кактана виновный оплачивал товары в присутствии работников торговли, которые какого-либо участия в осуществлении транзакций не принимали. Соответственно, Ю. Ю. Кактан в заблуждение никого не вводил, совершил хищение не путем обмана, а тайно.

Наука живо отреагировала на принятое решение по данному делу. И. А. Клепицкий, не соглашаясь с предлагаемой квалификацией, ссылается на то, что безналичные деньги вообще не могут выступать предметом кражи[1]. В свою очередь, С. В. Скляров, напротив, поддерживает позицию Верховного Суда Российской Федерации[2].

Анализируя мнения теоретиков и судебно-следственную практику, следует сделать вывод, что решение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации по делу Ю. Ю. Кактана в современных условиях является обоснованным. Исходя из обстоятельств преступления, совершенного Ю. Ю. Кактаном, понятно, что работники торговой организации, другие покупатели и иные лица хотя и присутствовали при совершении им преступления, но не осознавали противоправность его действий, а значит в его деянии присутствует та форма тайности, о которой нам говорит Пленум Верховного Суда Российской Федерации.

Другой вопрос, который еще не нашел своего однозначного разрешения, – какие в сложившихся условиях действия следует квалифицировать по ст. 159.3 УК РФ? В этой части практика пока не может продемонстрировать соответствующих примеров, а в теории нет однозначных рекомендаций и предложений. Высказываются суждения, что данная норма пополнит список так называемых мертвых норм, исключенных из области фактического правоприменения.

Модернизация диспозиции ст. 159.3 УК РФ, а также анализируемое решение по делу Ю. Ю. Кактана кардинально изменят сложившуюся правоприменительную практику. Современные формы дистанционного мошенничества с использованием ЭСП

---

[1] Клепицкий И. А. Кража безналичных денег: простой ответ на простой вопрос // Уголовное право. 2020. № 5. С. 87.

[2] Скляров С. В. Обман при хищении // Уголовное право. 2020. № 5. С. 107.

(без признаков деструктивного вмешательства в их функционирование) с высокой долей вероятности будут получать оценку по ст. 159.3 УК РФ. Таким образом, хищения, совершаемые с использованием сайтов-ловушек популярных интернет-магазинов благотворительных организаций и т. п., будут получать оценку не в рамках общеуголовного мошенничества (как указывает о том Пленум Верховного Суда Российской Федерации в постановлении от 30 ноября 2017 г. № 48), а как мошенничество с использованием ЭСП[1].

[1] Русскевич Е. А. Конкуренция уголовно-правовых норм при квалификации хищений с банковского счета потерпевшего, а равно в отношении электронных денежных средств // Вестник Университета прокуратуры Российской Федерации. 2019. № 4 (72). С. 29–33.

ГЛАВА 4. Оперативно-разыскная характеристика дистанционных хищений безналичных денежных средств граждан, совершаемых в сфере информационных технологий

§ 4.1. Общие положения оперативно-разыскной характеристики дистанционных хищений безналичных денежных средств граждан, совершаемых в сфере информационных технологий

В последние годы борьба с преступлениями в сфере информационно-телекоммуникационных технологий приобрела особую остроту и стала выделяться в качестве одного из приоритетных направлений в работе органов внутренних дел. Сложность оперативной обстановки в этой сфере связывают с развитием научно-технического прогресса, доступностью подключения к глобальной сети «Интернет», невысокой стоимостью интернет-услуг и мобильной связи, низкой грамотностью населения в вопросах информационных технологий и нерешенностью ряда правовых проблем в этой сфере. При этом в основе значительного увеличения количества преступлений в сфере информационных технологий и разнообразия способов их совершения лежит анонимность пользователей сети «Интернет», мобильной связи и наличие программных инструментов дистанционного перераспределения материальных благ (банкоматы (АТМ), терминалы самообслуживания (ІТТ), POS-терминалы, интернет-банк, мобильный банк, системы ДБО и др.).

Статистические показатели зарегистрированных хищений в сфере информационных технологий свидетельствуют об их

устойчивом росте, что связано с тенденцией увеличения в целом преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий.

По словам сотрудников практических органов, латентность дистанционных хищений в сфере информационно-телекоммуникационных технологий чрезвычайно высока и по косвенным признакам превышает в несколько раз сведения официальной статистики. Причины, по которым потерпевшие от этих преступлений граждане не обращаются в правоохранительные органы, различны. Как правило, это происходит вследствие незначительности причиненного им ущерба, нежелания втягиваться в бюрократические процедуры уголовного судопроизводства, возникшего ощущения стыда и неловкости, из-за осознания собственной глупости и чрезмерной доверчивости и др.

Дистанционные хищения безналичных денежных средств, совершаемые с использованием компьютерных и телекоммуникационных технологий, относятся к категории технически сложных по замыслу и исполнению преступлений. Для их осуществления преступники часто объединяются в группы с четким распределением ролей в процессе подготовки и реализации преступного замысла. Организаторы и исполнители нередко обладают высокой квалификацией и глубокими знаниями в области информационных технологий, психологии, банковского обслуживания клиентов и др. По этой причине органам внутренних дел особенно важно противопоставить их действиям своевременные и квалифицированные меры по выявлению, пресечению и предупреждению преступных посягательств в этой сфере, их разоблачению и привлечению виновных к уголовной ответственности. При этом раскрытие дистанционных хищений в сфере информационных технологий в первую очередь ложится на плечи подразделений уголовного розыска, которым приходится испытывать большие трудности на этом поприще.

В настоящее время известно множество различных видов дистанционных хищений безналичных денежных средств граждан с использованием информационно-телекоммуникационных технологий. Механизм их совершения характеризуется тем, что преступники не вступают в непосредственный контакт с потерпевшими. Это значительно усложняет раскрытие и расследование таких преступлений, так как потерпевший впоследствии не может воспроизвести признаки внешности преступника. Специфика состоит еще и в том, что в отличие от преступлений, которым присущ физический способ воздействия на потерпевшего, при дистанционных хищениях в сфере информационно-телекоммуникационных технологий способ воздействия на потерпевшего носит дистанционный характер и строится на особых доверительных отношениях, сложившихся между потерпевшим и преступником благодаря умелому применению последним приемов социальной инженерии.

Социальная инженерия – это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным[1].

Представляется, что для грамотного планирования и организации раскрытия и расследования дистанционных хищений безналичных денежных средств граждан, совершаемых с использованием информационно-телекоммуникационных технологий, практическим сотрудникам требуется детально уяснить структуру данных преступлений, понимать механизм преступных действий, а для этого им необходимо ознакомиться с подробной классификацией современных способов их совершения. Ведь

[1] В сфере информационной безопасности данный термин был популяризован в начале XXI в. бывшим компьютерным преступником, ныне консультантом по безопасности, Кевином Митником, который утверждал, что самое уязвимое место любой системы безопасности – человеческий фактор (см.: Социальная инженерия // URL: https://ru.wikipedia.org/wiki/Социальная_инженерия#Мошенничество_с_использованием_брендов_известных_корпораций).

давно известно, что изучение способов совершения преступлений служит ценным источником сведений, необходимых для разработки средств, приемов и методов раскрытия, расследования и предупреждения преступлений[1].

В теории оперативно-разыскной деятельности информация о способе совершения преступлений является важным элементом оперативно-разыскной характеристики преступлений, составляющим ее «ядерное» содержание. При этом способы рассматриваются не только и не столько с точки зрения уголовно-правовой квалификации, как с точки зрения последовательности совершаемых преступниками действий, что имеет принципиальное значение для качественного документирования оперативными подразделениями их преступной деятельности.

В самом общем виде способы совершения наиболее распространенных дистанционных хищений безналичных денежных средств у граждан, совершаемых в сфере информационно-телекоммуникационных технологий, по которым проведение оперативно-разыскных мероприятий осуществляется силами подразделений уголовного розыска территориальных органов внутренних дел, можно разделить на два вида:

1. Дистанционные хищения безналичных денежных средств граждан с использованием средств мобильной телефонной связи (телефонные кражи и телефонные мошенничества).

2. Дистанционные хищения безналичных денежных средств граждан с использованием сети «Интернет» (интернет-кражи и интернет-мошенничества).

[1] Зуйков Г. Г. Поиск преступников по признакам способов совершения преступлений : учебное пособие. М. : ВШ МВД СССР, 1970. С. 4.

§ 4.2. Оперативно-разыскная характеристика распространенных дистанционных хищений безналичных денежных средств граждан, совершаемых с использованием средств мобильной телефонной связи

Для совершения дистанционных хищений безналичных денежных средств у граждан с использованием средств мобильной телефонной связи преступники используют сотовую или проводную стационарную связь, контактируя с потерпевшими посредством живого разговора по телефону или посредством SMS-сообщений. Наиболее часто встречаются следующие способы дистанционных хищений с использованием телефонной связи, которые условно называются:

1. Телефонные хищения безналичных денежных средств граждан под видом блокировки их банковской платежной карты (далее – БПК) или несанкционированного списания с нее средств (SMS-кражи и SMS-мошенничества)[1].

[1] В соответствии с разъяснениями Верховного Суда Российской Федерации «когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража» (см.: ч. 3 п. 17 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»). Несмотря на это, анализ способов совершения преступлений данного вида показывает, что часто преступники не ограничиваются выяснением только лишь реквизитов БПК или персональных данных потерпевшего. Например, используя преступную схему с удаленной перерегистрацией интернет-банка потерпевшего, злоумышленники до окончания преступления (т. е. вплоть до перевода денежных средств с вкладов и счетов потерпевшего) находятся с ним на связи. В ряде способов они прямо сообщают потерпевшему о намерении перевода денег с его БПК, он это осознает, но по разным причинам продолжает доверять преступникам. В связи с тем, что обман в указанных случаях направлен непосредственно на завладение чужим

2. Телефонные хищения денежных средств граждан под видом возникших проблем с законом у их родственника.

3. Телефонные хищения безналичных денежных средств пожилых людей, пенсионеров, обманутых дольщиков, льготников и других незащищенных слоев населения под видом различных социальных выплат или компенсаций.

Рассмотрим подробно каждый из перечисленных способов.

В первом случае человек, имеющий в своем распоряжении БПК, получает SMS-сообщение, содержащее телефон для обратной связи. Наиболее распространенными вариантами таких сообщений являются:

– «Ваша карта VISA заблокирована. Справка по тел.: 8 960 848-88-85. ЦБ РФ»;

– «Уважаемый клиент, с вашей банковской карты списано 9800.60 руб. Инф.: 8 800 555-20-10»;

– «Операции по вашей карте приостановлены. Обращаться по тел.: 8 800 555-33-55»;

– «Оплата услуг на сумму 7 380 руб. произведена успешно. Инф.: 8 951 270-09-35»;

– «Оплата покупки с вашей банковской карты на сумму 13 700 руб. успешно зарезервирована (OZON.ru). Платеж будет проведен в течение суток. Если вы не совершали покупку, срочно свяжитесь со службой поддержки: 8 800 555-33-55».

Причем в качестве телефона для обратной связи может быть указан многоканальный федеральный бесплатный номер (например, 8 800 555-05-50, 8 800 505-55-05, 8 800 550-55-50 и др.)[1].

Человеку, перезвонившему на указанный в сообщении номер, злоумышленники представляются сотрудниками службы

имуществом, полагаем, что действия преступников по-прежнему будут образовывать состав мошенничества (см.: ч. 3 п. 2. указанного постановления).

[1] Сегодня данные номера доступны для приобретения не только юридическим, но и физическим лицам (см., например: Тарифы компании AnTelecom. URL: https://an-telecom.ru/tarifyi).

безопасности банка или платежной системы, специалистами службы технической поддержки или контактного центра.

Преступники вводят человека в заблуждение и вытягивают из него информацию относительно реквизитов его БПК.

Нередко уже на этом этапе преступники пытаются провести регистрацию (перерегистрацию) интернет-банка потерпевшего. Для этого они в интернете открывают официальную страницу сервиса удаленной регистрации интернет-банка[1] и вводят туда номер БПК потерпевшего. Владельцу БПК на привязанный к ней телефон приходит цифровой пятизначный SMS-пароль, который преступники под разными предлогами выуживают у потерпевшего с помощью приемов социальной инженерии и в течение двух минут осуществляют перерегистрацию интернет-банка потерпевшего, установив новый логин и пароль.

Преодолев систему безопасности только одной БПК потерпевшего и войдя в интернет-банк, преступники получают доступ ко всем его счетам и вкладам. При этом похитить деньги с вклада или счета становится для них приоритетной задачей, так как на них, как правило, имеется более внушительная сумма, нежели на платежной карте.

Для хищения средств со счетов и вкладов также применяются методы социальной инженерии и сначала для отвода глаз преступники зачисляют деньги на БПК самого потерпевшего. Это делается для того, чтобы потерпевший поверил в якобы произошедший системный сбой и следовал инструкциям «лжеоператоров» банка. Кроме того, такая схема позволяет обойти систему фрод-мониторинга банка, делая компьютер злоумышленников доверенным в системе ДБО.

Потом преступники перезванивают потерпевшему и под предлогом произошедшего банковского системного сбоя просят

---

[1] См., например: официальная страница интернет-сервиса удаленной регистрации «Сбербанк Онлайн». URL: https://online.sberbank.ru/CSAFront/async/page/registration.do ; Как быстро зарегистрироваться в «Сбербанк Онлайн» в 3 шага // URL: https://www.youtube.com/watch?v=Opa7rXsArqM.

вернуть поступившие клиенту деньги назад в банк, передав «оператору» приходящие на телефон пароли. Если им это удается, то денежные средства потерпевшего незамедлительно переводятся на подконтрольные преступникам БПК, банковские счета и балансы мобильных телефонных номеров.

В случае, когда по какой-то причине преступники отказываются от схемы с регистрацией (перерегистрацией) интернет-банка, они в убедительной форме предлагают потерпевшему срочно провести действия по разблокировке карты, отмене перевода, возврату зарезервированных средств и т. п. Следуя получаемым по телефону инструкциям, потерпевшие:

– подключают мобильный банк на телефон мошенников;
– сообщают им реквизиты других своих БПК;
– сообщают им логины и пароли от интернет-банка;
– сами отправляют со своего телефона SMS-оферты для подтверждения операций.

В итоге сбережения потерпевших преступники переводят на подконтрольные себе электронные платежные сервисы, БПК, банковские счета, лицевые счета телефонных номеров или используют для покупок в интернет-магазинах, интернет-казино, игровых интернет-платформах и др.

Схема телефонных хищений денежных средств граждан под видом возникших проблем с законом у их родственника, как правило, выглядит следующим образом.

Преступник путем случайного набора номера звонит на мобильный или домашний стационарный телефон незнакомому человеку (стараясь выбирать граждан пожилого возраста) и представляется ему близким родственником (сыном, внуком) либо сотрудником правоохранительных органов (следователем, оперуполномоченным, сотрудником ГИБДД и т. п.), задержавшем его близкого родственника.

Далее преступник под видом запуганного родственника, изменив голос (например, произнося слова полушепотом, с хри-

потцой или с нотками страха), или незнакомого сотрудника правоохранительного органа сообщает потерпевшему, что у него самого (если представляется родственником) или у его родственника (если представляется сотрудником) возникли проблемы с законом (он устроил дорожно-транспортное происшествие, сбил человека, задержан с наркотиками, находился за рулем в нетрезвом виде и др.), однако еще есть возможность их уладить, заплатив определенную денежную сумму.

Если потерпевший соглашается дать взятку за непривлечение «родственника» к уголовной или административной ответственности, то преступник указывает способы передачи или перечисления денег (нарочно или путем безналичного перевода).

Если преступник настаивает на передаче денег нарочно, то за ними, как правило, приезжает таксист (курьер), который забирает деньги и в дальнейшем (все или их часть) передает (переводит) непосредственно инициатору преступления, его родственникам либо иным лицам, рекомендованным преступником при разговоре с таксистом (курьером) по телефону.

Если преступник предлагает безналичный перевод, то в этом случае деньги переводятся на подконтрольные ему номера телефонов (иногда нескольких), БПК, электронные кошельки («Яндекс.Деньги», WebMoney, Qiwi, «МОБИ.деньги» и др.), криптовалютные кошельки или путем почтовых или банковских переводов (например, по системе «Блиц-перевод», «Юнистрим», WesternUnion, «Золотая корона» и др.).

В случае перевода денежных средств на номера телефонов далее осуществляется их перевод на подконтрольный банковский счет или на номер БПК, что предусмотрено всеми операторами сотовой связи в рамках услуги «Мобильные переводы».

Подельник преступника, осуществивший снятие денежных средств с банковского счета или с БПК, используя банкомат, терминал самообслуживания, интернет-банк, осуществляет перевод

денежных средств (всех или их часть) преступнику или его родственникам[1].

Схема телефонных хищений безналичных денежных средств пожилых людей, пенсионеров, обманутых дольщиков, льготников и других незащищенных слоев населения под видом различных социальных выплат или компенсаций выглядит следующим образом.

Преступники связываются с пожилым человеком, пенсионером, обманутым дольщиком, льготником или иным лицом из числа незащищенных слоев населения, позвонив ему на стационарный городской домашний (мобильный) телефон, и представляются сотрудниками Пенсионного фонда Российской Федерации (ПФР), Банка, службы социальной защиты населения, ОВД, прокуратуры или иных правоохранительных органов.

Человеку предлагают получить единовременную социальную выплату или компенсацию, например по следующим причинам:

– он попадает под действие государственной программы «Дети войны» и ему положена путевка в санаторий и единовременная денежная выплата в размере от 200 до 500 тыс. руб.;

– он не пользуется социальными пособиями и ему полагается компенсация;

– он когда-то уже пострадал от мошенников, их поймали и теперь возвращают деньги.

---

[1] В результате проведенного в ГУУР МВД России анализа было выявлено, что в 60 % случаев преступники совершают данные преступления находясь в местах лишения свободы. Большинство преступлений данной направленности совершалось осужденными, отбывающими наказание в исправительных учреждениях ФСИН России по Курганской (ИК-6), Самарской (ИК-28), Новосибирской (ИК-21) областям и в Ханты-Мансийском автономном округе (ИК-11) (См., подробнее: Памятка следователю о проведении проверки и расследовании уголовных дел по фактам мошенничеств с использованием мобильных средств связи : Подготовлена контрольно-методическим управлением Следственного департамента МВД России с использованием материалов ГСУ ГУ МВД России по Кемеровской области, СУ УМВД России по Белгородской области и ГУУР МВД России в 2015 г.).

У злоумышленников, как правило, уже имеется начальная информация об объекте преступной атаки (чаще всего это: Ф. И. О., дата рождения, адрес, телефон; сведения, что тот ранее уже становился жертвой мошенников, и др.). Данную информацию преступники получают:

– из открытых источников в сети «Интернет»;

– используя утечку из правоохранительных органов;

– используя утечку из Пенсионного фонда Российской Федерации, органов социальной защиты населения, государственных и коммерческих учреждений здравоохранения и других источников.

Для получения обещанной социальной выплаты или компенсации человек следует указаниям злоумышленников:

– сообщает номер своей БПК, а если карты нет, то оформляет ее;

– подключает услугу «Мобильный банк» и «привязывает» к своей БПК телефон преступников;

– сообщает свои персональные данные;

– сообщает преступникам логины и пароли входа в интернет-банк, в том числе в его мобильное приложение, SMS-коды для регистрации интернет-банка и перевода средств, CVV2 (CVC2) коды и т. д.

В результате злоумышленники получают полный доступ к системе интернет-банка и проводят несанкционированные операции с вкладов и карт клиента.

В случае, когда у потерпевших нет оформленных БПК или средств на них, преступникам удается выманить от 30 до 70 тыс. руб., под видом оплаты 13 % налога на доходы. Как правило, потерпевших просят перевести деньги на подконтрольный счет (БПК) или отдать их на руки «работникам Пенсионного фонда, социальных служб» и т. д.

§ 4.3. Оперативно-разыскная характеристика распространенных дистанционных хищений безналичных денежных средств граждан, совершаемых с использованием сети «Интернет»

Для совершения дистанционных хищений безналичных денежных средств у граждан, совершаемых с использованием сети «Интернет», преступники используют различные интернет-платформы (социальные сети, форумы сайтов, интернет-магазины), контактируя с потерпевшими посредством электронной переписки, а в ряде случаев, используя сотовую связь на последующих этапах криминальных схем. Наиболее часто встречаются следующие способы краж и мошенничеств с использованием сети «Интернет»:

1. Интернет-хищения безналичных денежных средств граждан на российских торговых интернет-площадках бесплатных объявлений.

2. Интернет-хищения безналичных денежных средств граждан в интернет-магазинах.

3. Интернет-хищения безналичных денежных средств граждан в социальных сетях и Skype.

Рассмотрим подробно каждый из перечисленных способов.

Первый способ делится на два варианта:

1. «Преступник – покупатель».

Добропорядочный человек размещает объявление на подходящем сайте (Avito, Avto.ru, Am.ru, Drom.ru, CarPrice, «Из рук в руки» и др.) о продаже какого-либо товара. Ему поступает звонок якобы от потенциального покупателя, который готов приобрести данный товар, но предоплату или полную сумму хочет внести переводом на БПК, для чего запрашивает ее номер. Если продавец соглашается и сообщает номер БПК, то далее возможны следующие варианты развития событий:

– злоумышленники заходят на страницу удаленной регистрации интернет-банка, вводят в открывшуюся веб-форму номер сообщенной потерпевшим БПК и обманом выуживают у него пароли, приходящие на телефон, подключенный к Мобильному банку. Необходимость сообщить пароли они объясняют, например, тем, что перевод осуществляется со счета коммерческого банка, а не с БПК, и поэтому перевод не проходит, пока не будет получено подтверждение паролем из SMS, пришедшей на телефон получателя платежа. Если человека удается таким образом обмануть, то денежные средства с его карт и вкладов похищаются посредством перевода на банковские счета, БПК или счета телефонных номеров;

– преступники внушают человеку, что для успешного перевода средств необходимо сделать номер их телефона доверенным перед банком, для чего просят проделать эту процедуру с банкомата. Введенный таким образом в заблуждение человек сам подключает мобильный банк на телефон мошенников. Преступники регистрируются в интернет-банке и похищают средства потерпевшего с его БПК и вкладов;

– преступники совершают онлайн-покупку на крупную сумму, используя реквизиты карты потерпевшего (номер карты, CVV2 (CVC2) код, срок действия карты, имя владельца), которые он сам им сообщил;

– преступники обманом выуживают у человека логины и пароли входа в интернет-банк и похищают средства с его БПК и вкладов.

2. «Преступник – продавец».

Преступники сами размещают объявление на подходящей торговой интернет-площадке (о сдаче жилья, продаже машины, квартиры, антиквариата или любого другого предмета), указывают телефон и (или) адрес электронной почты для обратной связи и ждут потенциального добросовестного покупателя (клиента). Характерной особенностью привлечения потенциальных

клиентов является указание в объявлении самой низкой рыночной цены, обещание бесплатной доставки и другие неоспоримые преимущества, создающие впечатление максимальной выгоды.

Когда поступает звонок от лица, готового приобрести товар, ему предлагается внести предоплату или полную сумму переводом на банковский счет, БПК, электронный кошелек или на счет телефонного номера. Показывать товар злоумышленники под разными предлогами отказываются и предлагают переслать фотографию товара на электронную почту.

Преступник и потерпевший могут некоторое время вести электронную переписку, при этом преступник, как правило, демонстрирует потерпевшему фотографии товара. Стараясь убедить покупателя в своей надежности и качестве товара, злоумышленники могут долго оговаривать цену, способ оплаты, сроки и условия доставки.

В качестве распространенного предлога невозможности осмотра товара вживую сообщается, что собственник находится в другом городе, в командировке, переехал на постоянное место жительства за границу и др. Необходимость внесения предварительной оплаты объясняется большим спросом на предмет аренды или продажи, и скорейшая предоплата только подтвердит серьезность намерений именно этого клиента.

Получив предоплату или всю оговоренную сумму, преступники удаляют объявление с интернет-площадки, не отвечают на звонки потерпевшего, а позже совсем отключают телефон.

Бывали случаи, когда несмотря на внесенную предоплату, преступники под различными предлогами просили перевести еще денег. Например, в назначенный день встречи (передачи товара, услуги) сообщали, что не смогут приехать, так как им не выплатили зарплату, их машина сломалась и нужны деньги на такси, на ремонт машины и пр. Примечательно, что преступники, промышляющие этим способом, не гнушаются даже небольших сумм от одной до пяти тыс. руб., что является лишним

подтверждением участия в этом лиц, находящихся в местах лишения свободы или недавно освободившихся, не имеющих постоянного источника дохода.

При втором способе краж и мошенничеств в сети «Интернет» преступники создают в интернете сайт под видом интернет-магазина, в котором предлагают клиентам различный ассортимент популярных товаров. Особенностью привлечения потенциальных клиентов является указание самой низкой рыночной цены, обещание бесплатной доставки и другие неоспоримые преимущества, создающие впечатление максимальной выгоды.

Добросовестный покупатель в поисках нужного товара обнаруживает в интернете мошеннический сайт и решает сделать в нем заказ. Для этого он регистрируется на сайте, указывает свои паспортные данные, мобильный телефон, заказывает доставку и др.

Потенциальный покупатель получает от магазина электронное письмо с подтверждением заказа и счетом на предварительную оплату товара, в котором указаны реквизиты банка, БПК или универсального электронного платежного сервиса.

В некоторых случаях покупатель перезванивает на телефонные номера, указанные на сайте либо в электронных письмах. Злоумышленники убеждают его в том, что заказ принят, оговаривают сроки и условия доставки и прочие вопросы, создавая у потенциального клиента впечатление надежности интернет-магазина.

Решив внести предварительную оплату, покупатель перечисляет денежные средства на указанный ему банковский счет, БПК или электронный кошелек.

Некоторое время после перечисления потерпевшим денежных средств с целью сокрытия следов своей преступной деятельности злоумышленники отвечают потерпевшему на его звонки и электронные письма, убеждают клиента в выполнении своих обязательств, объясняя задержку доставки товара различными непредвиденными обстоятельствами (задержками на таможне,

проблемами у поставщика, большим количеством заказов, блокировкой банковских счетов, ожиданием поставки указанной покупателем комплектации и др.).

Обманув достаточное количество клиентов, преступники перечисляют денежные средства с промежуточных банковских счетов и платежных сервисов на другие банковские счета, БПК, после чего обналичивают их и прекращают всякое взаимодействие с потерпевшими.

Третий способ интернет-хищений, как и первый, делится на два варианта:

1. «От имени друга».

Преступники взламывают личный кабинет пользователя в социальных сетях или Skype и от его имени рассылают его друзьям (контактам) сообщения с различными просьбами. Наиболее часто встречаются следующие варианты подобных сообщений:

– преступники просят одолжить денег, перечислить деньги по интернету, оплатить телефон своего «родственника» и т. д. Предлоги находятся самые разные: он заболел, его уволили, он попал в аварию, ему срочно нужно оплатить интернет, у его родственника закончились деньги на телефоне, ему нужно пополнить счет БПК, а сделать это негде и т. д.

Если человек соглашается, ему приходит сообщение с номером БПК или номером телефона, подконтрольных злоумышленникам, на которые он должен перевести указанную сумму. Спустя некоторое время потерпевший узнает от друга, что его аккаунт в социальной сети (или в Skype) был взломан и он не просил ни о какой материальной помощи;

– преступники просят срочно помочь вывести деньги с Яндекс-кошелька или с БПК на карту Сбербанка, которой у них якобы нет. В качестве причины сообщают, что деньги могут сгореть, так как истекает срок действия Яндекс-кошелька (БПК). Если человек соглашается, то преступники запрашивают у него номер БПК Сбербанка, остальные ее реквизиты, приходящие

на телефон SMS-коды или логин и пароль для входа в Сбербанк Онлайн, после чего похищают средства со счетов и вкладов потерпевшего;

– преступники сообщают «другу», что потеряли свой телефон или он сломался, и просят «друга» срочно прислать свой номер телефона в ответном сообщении, так как все контакты телефонной книги были утеряны вместе с телефоном. Срочность объясняют тем, что должны получить от третьего лица важное SMS-сообщение, а так как их телефон утерян (сломан), то просят у «друга» разрешения прислать сообщение на его номер. Также злоумышленники просят «друга» сразу после получения сообщения от третьего лица переслать его им через социальную сеть (Skype). В результате активации злоумышленниками кода подтверждения, полученного в сообщении от потерпевшего, у последнего с телефона автоматически списываются разные денежные суммы;

– преступники просят «друга» открыть сюрприз, отправив SMS на четырехзначный номер, иначе тот якобы обидится. В результате звонка или отправки потерпевшим SMS на этот номер у него со счета телефона списывается определенная сумма денег, часто в размере 300–500 руб.

Нужно подчеркнуть, что совершение преступления указанными способами невозможно без предварительного фишинга[1] или хакинга[2], направленного на взлом аккаунтов социальных сетей или Skype.

2. «От имени сотрудника банка».

---

[1] Фишинг (англ. phishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям (см.: URL: https://ru.wikipedia.org/wiki/Фишинг).

[2] Хакинг – внесение изменений в программном обеспечении, для достижения определенных целей, отличающихся от целей создателей программ, очень часто изменения являются вредоносными. (см.: Что такое хакинг и как от него обезопасить свой компьютер? // URL: http://procomputer.su/comp-gramotnost/164-chto-takoe-khaking-i-kak-obezopasit-kompyuter).

Преступники создают аккаунт в социальных сетях, который по стилистике и содержанию выглядит как страница сотрудника банка. Различными способами они находят клиентов банка (например, просматривая ленты официальной группы банка) и предлагают им помощь или консультационные услуги от имени банка. Под предлогом соблюдения формального требования перед консультацией клиента «псевдоконсультанты» запрашивают у него все необходимые данные для регистрации в интернет-банке и проведения операций в сети «Интернет». Способ рассчитан на клиентов банка в возрасте, зарегистрированных в социальных сетях (как правило, в «Одноклассниках»), имеющих счета в банках, пенсионные (зарплатные) БПК, но которые не пользуются мобильным и интернет-банкингом. Под предлогом ликбеза и просвещения в вопросах использования всех возможностей и удобств интернет-банкинга, человека обманывают, получают доступ к его интернет-банку и похищают средства с его счетов и вкладов.

Полагаем, что знание курсантами, слушателями и практическими сотрудниками механизма совершения указанных преступлений и детальное уяснение нюансов в способах их совершения позволят предотвратить с их стороны возможное совершение ошибок в документировании данных преступлений на практике и в целом повысят готовность органов внутренних дел в оказании должного противодействия преступности в сфере информационно-телекоммуникационных технологий.

ГЛАВА 5. Организационно-тактические и уголовно-процессуальные вопросы расследования преступлений в сфере информационных технологий

§ 5.1. Деятельность на стадии возбуждения уголовного дела при расследовании преступлений в сфере информационных технологий

В настоящее время нет общепризнанного определения понятия преступлений в сфере информационных технологий, соответственно отсутствует статистика этих преступлений. Однако, по данным ведомства, есть показатели количества преступлений в сфере компьютерной информации и преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий.

В 2020 г. сохранилась динамика существенного роста количества преступлений рассматриваемой категории, уголовные дела о которых находились в производстве правоохранительных органов Российской Федерации: 580,26 тыс., что на 73,4 % превышает показатель предыдущего года (339,3 тыс.), непосредственно в отчетном периоде зарегистрировано 510,4 тыс. – это на 73,4 % превышает показатель предыдущего года (294,4 тыс.). Сложившиеся обстоятельства социально-экономического характера, обусловленные распространением и преодолением последствий новой коронавирусной инфекции COVID-19, создали дополнительные условия для усиления криминальной активности, связанной с использованием информационных технологий.

В массиве уголовных дел данной категории, зарегистрированных в 2020 г., 75,2 % составляют дистанционные хищения,

совершенные с банковских карт, с использованием сети «Интернет» и средств мобильной связи, квалифицируемые по ст.ст. 158 и 159 УК РФ.

В общем числе зарегистрированных преступлений удельный вес преступлений в сфере информационных технологий увеличился с 14,5 % в 2019 г. до 25,0% в 2020 г.

Раскрываемость таких преступлений по-прежнему невысока и по итогам 2020 г. составила 18.6 % (–16 % к АППГ – 22,2 %).

В отчетном периоде зафиксирована положительная динамика по направлению уголовных дел в суд. Так, в 2020 г. количество преступлений, расследованных следователями органов внутренних дел с направлением дел в суд, составило 80,531 тыс. (+89,6 % к АППГ – 42,470 тыс.).

Наиболее широкое распространение в настоящее время получили преступные деяния с использованием банковских карт, сети «Интернет», средств мобильной связи и компьютерной техники.

Получили распространение мошенничества, сопровождающиеся внесением в единые государственные реестры фиктивных сведений о юридических лицах и индивидуальных предпринимателях, в результате которых злоумышленники приобретают возможность завладения имуществом, активами физических и юридических лиц.

Значительное число «дистанционных мошенничеств» совершается лицами, отбывающими наказания в местах лишения свободы.

Большое количество краж данного вида совершено с использованием мобильной связи, банковских карт и компьютерной техники.

Рассматриваемые преступления все чаще совершаются технически оснащенными преступными группами (в том числе международными), характеризуются усложненными способами их подготовки и сокрытия, созданием и использованием вредоносных компьютерных программ.

Наиболее распространенными способами совершения таких преступлений являются:

– хищения денежных средств и иного имущества с использованием компьютерных технологий (кражи из электронных кошельков, с банковских счетов физических и юридических лиц, с помощью накладок на банкоматы);

– неправомерный доступ к охраняемой законом компьютерной информации;

– применение вредоносных программ с целью незаконного использования объектов авторского права, в том числе прав на программное обеспечение;

– хищения путем заражения систем ДБО, выставления поддельных POS-терминалов, атак на мобильные устройства, брокерские системы в сети «Интернет» и банки;

– использование методов социальной инженерии, в результате чего потерпевшие самостоятельно предоставляют злоумышленникам реквизиты своих банковских карт, конфиденциальную информацию, а также паспортные данные, позволяющие провести идентификацию и совершить хищение денежных средств[1].

Специфика стадии возбуждения уголовного дела обусловлена особенностью конкретного вида преступления, что определяет последовательность действий следователя (дознавателя) при обнаружении признаков такого преступления. Выявленные признаки оказывают влияние на выбор сил и средств, а также ход всего дальнейшего расследования.

В соответствии с требованиями закона решение о возбуждении уголовного дела любой категории возможно лишь при наличии соответствующего повода и оснований.

---

[1] Информационно-аналитические материалы Следственного департамента МВД России за 2017–2020 гг. // URL: https://xn--b1aew.xn--p1ai/mvd/-sovorg/prav_kom/other_documents.

В соответствии с ч. 1 ст. 140 УПК РФ поводами для возбуждения уголовного дела служат: 1) заявление о преступлении; 2) явка с повинной; 3) сообщение о совершенном или готовящемся преступлении, полученное из иных источников; 4) постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании.

Анализ следственно-судебной практики и научных работ позволяет сделать вывод, что типичными поводами по данной категории преступлений являются:

1) заявление от граждан – физических лиц или представителей юридических лиц (около 80 %);

2) сообщение о совершенном или готовящемся преступлении, полученное из иных источников, оформленное рапортом об обнаружении признаков преступления, составляемым сотрудником органа дознания или следователем, осуществляющим проверку сообщения о преступлении (около 20 % соответственно)[1].

В соответствии с ч. 2 ст. 140 УПК РФ основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления.

Следует помнить, что в уголовно-процессуальном законе отсутствует требование об обязательности выяснения уже на стадии возбуждения уголовного дела всех обстоятельств происшедшего события, содержащего признаки преступления. На данной стадии достаточно установить факты, указывающие на наличие признаков преступления. Выяснение же конкретных обстоятельств преступления и лиц, виновных в его совершении, возможно

[1] Расследование неправомерного доступа к компьютерной информации. учебное пособие / под ред. Н. Г. Шурухнова. М. : Московский университет МВД России, 2004. С. 173 ; Коломинов В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. … канд. юрид. наук. Иркутск, 2017. С. 88.

после возбуждения уголовного дела в ходе предварительного расследования[1].

Как правило, на стадии возбуждения уголовного дела складываются следующие типичные ситуации:

– заявители (представители юридического лица, собственник или законный пользователь компьютерной информации) сами выявили факт преступления или признаки совершенного преступления, но не смогли установить лиц, его совершивших, и обратились в правоохранительные органы;

– заявители (представители юридического лица, собственник или законный пользователь компьютерной информации) не только обнаружили факт совершенного преступления, его признаки, но и выявили данные заподозренного лица (чаще всего это IP- или MAC-адрес ЭВМ, номер SIM-карты или абонентский номер мобильного телефона).

Решая вопрос о возбуждении уголовного дела рассматриваемой категории, следует отметить, что из-за значительного количества разновидностей подобных преступлений, основания возбуждения уголовных дел будут отличаться.

В последнее время при совершении преступлений в сфере информационных технологий, как уже было указано, все чаще используются методы социальной инженерии в системах ДБО.

Рассмотрим деятельность сотрудников правоохранительных органов на стадии возбуждения уголовного дела при проверке поступившей информации:

В рамках проверки сообщения о хищении с применением систем ДБО необходимо выяснить следующие обстоятельства:

– способ подготовки, совершения и сокрытия хищения;

---

[1] Обзор судебной практики Верховного Суда Российской Федерации. 2017. № 3 (утв. Президиумом Верховного Суда Российской Федерации 12 июля 2017 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_219925/.

– произошло ли списание денежных средств с банковского счета потерпевшего в результате действия, не связанного с хищением (ошибка, сбой программного обеспечения и т. п.);

– наличие/отсутствие вредоносных программ и их исходных текстов/файлов проектов на ЭВМ пострадавшего;

– сведения о лицах, причастных к хищению (Ф. И. О., имена учетных записей в программах для мгновенного обмена сообщениями, IP-адреса, данные о их социальных сетях, почтовые адреса и т. д.);

– наличие/отсутствие сведений об отправке, рассылке файлов вредоносного программного обеспечения и/или поддерживании сервисов, с помощью которых можно производить распространение вредоносных программ;

– наличие/отсутствие факта воздействия на сетевой ресурс для выведения его из строя и/или штатной работы;

– наличие/отсутствие сетевых запросов на ЭВМ пострадавшего, обработка которых привела к выведению данного ресурса из строя и/или штатной работы;

– сведения о лицах, причастных к созданию/использованию/распространению вредоносных компьютерных программ;

– сведения о лицах, программах, IP-адресах, которые могут быть причастны к отправке этих запросов в случае их обнаружения;

– наличие/отсутствие компьютерных программ для отправки большого количества сетевых запросов определенного формата;

– факт наличия/отсутствия следов запуска обнаруженных вредоносных компьютерных программ;

– сведения о сетевых ресурсах, на которые посылались сетевые запросы с помощью обнаруженных программ;

– наличие/отсутствие следов обращения к интернет-ресурсам, которые позволяют производить отправку большого количества сетевых запросов заданного формата на заданный сетевой ресурс;

– наличие/отсутствие следов обращения к атакуемому сетевому ресурсу с машины правонарушителя;

– причина, повлекшая реализацию DoS/DDoS атаки[1];

– наличие/отсутствие следов несанкционированного доступа к ЭВМ атакующего в определенный промежуток времени.

Проверка данных обстоятельств осуществляется сотрудником органа дознания и (или) следователем. Основными источниками информации, позволяющими выявить признаки преступления в сфере информационных технологий, обычно являются:

– заявление пострадавшего (его представителя) либо рапорт об обнаружении признаков преступления;

– протокол осмотра места происшествия;

– сопроводительное письмо руководителя органа дознания (о рассекречивании материалов ОРД);

– рапорт сотрудника об обнаружении признаков преступления;

– документы, фиксирующие этапы проведения оперативно-разыскных мероприятий (за исключением сведений, составляющих государственную тайну);

– объяснения лиц, имеющих доступ к ЭВМ потерпевшего (руководитель, бухгалтер, оператор, администратор и т. д.);

– документы, относящиеся к функционированию ЭВМ, имеющей доступ к системе ДБО потерпевшего и финансово-кредитной организации;

– объяснения сотрудников финансово-кредитной организации (в том числе сотрудников службы безопасности);

---

[1] DoS (Denial of Service, атака типа «отказ в обслуживании») – атака с целью довести атакуемую систему до отказа в обслуживании обращающихся к ней клиентов. DDoS (Distributed Denial of Service, распределенная атака типа «отказ в обслуживании») – атака с целью довести атакуемую систему до отказа в обслуживании обращающихся к ней клиентов, осуществляемая одновременно значительной группой правонарушителей.

– журналы регистрации событий (NetFlow), предоставляемые поставщиком интернет-услуг;

– журналы регистрации событий от кредитной организации, предоставляющей доступ в систему ДБО;

– протокол осмотра ЭВМ, с которых предположительно осуществлена DoS/DDoS атака;

– протокол осмотра ЭВМ, ноутбука, моноблока, смартфона, мобильного устройства, планшета и других средств потерпевшего, подключенных к системе ДБО;

– электронные носители информации («жесткие» диски, флеш-накопители (USB Flash, SSD), твердотельные гибридные накопители информации (SSHD), CD/DVD/Blu-ray диски и т. д.);

– материалы исследований и экспертиз содержимого HDD и иных электронных носителей информации, изъятых у заподозренного;

– сетевой ресурс (сервер/серверы, маршрутизатор, система обнаружения/предотвращения вторжений и т. д.)[1].

Указанные предметы и документы подлежат внимательному изучению с точки зрения их значения, для установления признаков преступления, соответствия требованиям закона, поскольку по результатам их изучения может быть принято решение о возбуждении уголовного дела, об отказе в возбуждении дела или о передачи сообщения по подследственности.

В случае возбуждения уголовного дела все обнаруженные и изъятые предметы (документы) могут иметь доказательное значение, поскольку могут быть отнесены к такому виду доказательств, который определяется законом как «иные документы» (п. 6 ч. 2 ст. 74 УПК РФ).

Следует отметить, что к числу наиболее специфических особенностей, характерных для стадии возбуждения уголовного

[1] Информационно-аналитические материалы Следственного департамента МВД России за 2015 г. // URL: https://xn--b1aew.xn--p1ai/mvd/sovorg/-prav_kom/other_documents.

дела по преступлениям в сфере информационных технологий относятся:

1. Обязательное участие специалиста при производстве процессуальных действий, предусмотренных ч. 1 ст. 144 УПК РФ. Например, при осмотре места происшествия, опросе киберпреступников, назначении компьютерно-технической экспертизы, осмотре и исследовании предметов и документов участие специалиста позволит обеспечить необходимое качество проведения данных процессуальных действий предотвратить утрату важной доказательственной информации.

Такими специалистами могут являться работники организаций, имеющие высокий уровень квалификации и работающие в области информационных технологий. Это могут быть и те, кто на профессиональном уровне осуществляет защиту информации, которую охраняет закон, например:

– сотрудники Федеральной службы по техническому и экспортному контролю, осуществляющие свою деятельность на основании Положения о Федеральной службе по техническому и экспортному контролю (утвержденному Указом Президента России от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»);

– специалисты компаний, обеспечивающие информационную безопасность (Лаборатория Касперского, Group-IB, BI.ZONE, Positive Technologies, Московский Исследовательский Центр Правительства Москвы и др.);

– специалисты, выполняющие судебные компьютерно-технические экспертизы;

– работники службы информационной безопасности различных организаций и учреждений;

– сотрудники научно-исследовательских и учебных заведений соответствующего профиля.

2. Обязательное проведение экспертиз, предметом исследования которых является изъятые по делу электронные носители

информации, ноутбуки, флэш-карты и т. д., с целью обнаружения вредоносного программного обеспечения иных сведений, имеющих значение для выявления признаков преступления (хотя ст. 196 УПК РФ не содержит требование обязательности назначения экспертиз по делам данной категории, однако это требование продиктовано спецификой процесса доказывания по такого рода делам).

3. Отсутствие заявления пострадавших (нередко лицо не подозревает, что в отношении него была попытка совершить хищение денежных средств с помощью информационных технологий. Например, внедренное преступниками вредоносное программное обеспечение подменило платежные реквизиты в осуществляемой транзакции, однако система «Фрод-мониторинга» и сотрудники службы безопасности финансово-кредитной организации заблокировали данную транзакцию). В подобных случаях атакуемое лицо даже не подозревает, что сотрудники кибербезопасности кредитной организации предотвратили хищение его денежных средств, что исключает личное обращение в правоохранительные органы. В свою очередь, сотрудники безопасности кредитной организации, соблюдая требования ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности», также не могут инициативно передавать в правоохранительные органы информацию о подобных инцидентах.

4. Отсутствие очевидцев, так как общение преступников осуществляется, как правило, в информационно-телекоммуникационной сети, нередко с использованием специальных программ, обеспечивающих анонимность такой коммуникации (анонимайзеров).

5. Менее обширная и более уязвимая доказательственная база в силу указанных выше причин.

6. Стремление заподозренного противодействовать расследованию путем выдвижения ложных версий, трудноопровергаемых объективными данными (таких как компьютер, с которого распространялось вредоносное программное обеспечение, принадлежит мне, однако кто в конкретное время им пользовался – затрудняюсь ответить; или в квартире установлен Wi-Fi роутер, кто им смог воспользоваться, я не знаю).

7. Взаимосвязь указанного рода преступлений с другими (подготавливаемыми или уже совершенными, так как нередко информационные технологии используются для совершения более тяжких преступлений. Так, осенью 2017 г. анонимные сообщения о заложенных бомбах поступали из разных городов России: Владивостока, Магадана, Омска, Челябинска, Уфы, Перми, Ставрополя, Москвы. Основной версией подобных звонков является спланированная атака с применением средств IP-телефонии. Такие системы позволяют организовать массовый обзвон из одного-двух мест и при этом скрыть реальный номер абонента[1]).

8. Наличие (как правило) состава преступления в действиях каждого лица, вовлеченного в криминальную деятельность, связанную с совершением преступлений в сфере информационных технологий (с вытекающими отсюда последствиями: криминальной круговой порукой указанных лиц, слабой свидетельской и доказательной базой по делам указанной категории, сложностью установления и доказывания связей между различными участниками преступных групп).

Еще один момент, который следует учесть при оценке первичных материалов о противоправных деяниях в сфере компьютерной информации, – это малозначительность деяния.

В ч. 2 ст. 14 УК РФ закреплено, что не является преступлением действие (бездействие), хотя формально и содержащее признаки

---

[1] Ложная тревога // URL: https://rg.ru/2017/09/12/reg-pfo/v-krupnyh-gorodah-rossii-evakuirovali-desiatki-shkol-vokzalov-i-tc.html ; Телефонные террористы дозвонились в Москву // URL: https://www.kommersant.ru /doc/3409928/.

какого-либо деяния, предусмотренного УК РФ, но в силу малозначительности не представляет общественной опасности.

Данным обстоятельством активно пользуются правонарушители, совершающие значительное количество мелких хищений, например по 100 руб. с каждого абонентского счета мобильного телефона. На первый взгляд малозначительность очевидна, но, когда с использованием вредоносного программного обеспечения совершаются тысячи таких хищений, восприятие ситуации меняется и о малозначительности говорить неуместно.

Перечисленные выше обстоятельства необходимо учитывать при выдвижении следственных версий по делам указанной категории, подготовке плана расследования, при выборе последовательности и тактики проведения дальнейших процессуальных действий.

§ 5.2. Уголовно-процессуальные основы досудебного производства по уголовным делам о преступлениях в сфере информационных технологий

При расследовании преступлений в сфере информационных технологий следователи и дознаватели сталкиваются как с организационными проблемами (длительность получения информации из различных регионов, небольшой срок хранения информации, нехватка экспертов по указанному профилю и другими), так и с целым рядом трудностей в толковании уголовно-процессуального законодательства, регламентирующего производство по уголовным делам.

Очевидно, в силу единства уголовно-процессуальной формы производство по уголовным делам о преступлениях в сфере информационных технологий, совершаемых против собственности, подчиняется общим правилам, тем не менее доказывание обстоятельств указанных преступлений все же обладает определенной

спецификой, прежде всего в части особенностей предмета доказывания.

Как известно, обстоятельства, подлежащие доказыванию, закреплены в чч. 1 и 2 ст. 73 УПК РФ и к ним относятся:

1) событие преступления (время, место, способ и другие обстоятельства совершения преступления);

2) виновность лица в совершении преступления, форма его вины и мотивы;

3) обстоятельства, характеризующие личность обвиняемого;

4) характер и размер вреда, причиненного преступлением;

5) обстоятельства, исключающие преступность и наказуемость деяния;

6) обстоятельства, смягчающие и отягчающие наказание;

7) обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания;

8) обстоятельства, подтверждающие, что имущество, подлежащее конфискации в соответствии со ст. 104.1 УК РФ, получено в результате совершения преступления или является доходами от этого имущества либо использовалось или предназначалось для использования в качестве орудия, оборудования или иного средства совершения преступления либо для финансирования терроризма, экстремистской деятельности (экстремизма), организованной группы, незаконного вооруженного формирования, преступного сообщества (преступной организации);

9) обстоятельства, способствовавшие совершению преступления.

При производстве по уголовным делам о преступлениях в сфере информационных технологий, совершаемых против собственности, должны быть установлены все перечисленные обстоятельства, однако наибольшая специфика присуща доказыванию обстоятельств, закрепленных в п. 1 ч. 1 ст. 73 УПК РФ –

«событие преступления» и в п. 2 ч. 1 ст. 73 УПК РФ – «виновность лица в совершении преступления».

Доказывание события преступления по уголовным делам о преступлениях в сфере информационных технологий, совершаемых против собственности, имеет ряд сложностей. Согласно п. 1 ч. 1 ст. 73 УПК РФ под событием преступления понимаются время, место, способ и другие обстоятельства совершения преступления.

1. **Время совершения преступления.** Хотя в ч. 2 ст. 9 УК РФ закреплено понятие времени совершения преступления – «время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий», однако при расследовании рассматриваемой категории уголовных дел нередко возникают случаи, когда конкретное время совершения преступления сложно установить, поскольку действие не носит никаких общественно опасных признаков, однако может считаться преступным.

К примеру, с целью совершения преступлений в сфере информационных технологий часто изготавливаются различные вредоносные компьютерные программы[1]. Сам процесс написания вредоносных компьютерных программ носит трудоемкий и длительный характер и часто связан с привлечением лиц, специализирующихся в области программирования.

Для написания сложных компьютерных программ, которые планируется использовать при совершении нескольких преступ-

[1] Вредоносная компьютерная программа – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации (см.: Информационный портал «Уголовный кодекс РФ». URL: http://www.ruukrf.ru).

лений, привлекается группа специалистов-программистов, причем каждый из них зачастую пишет лишь часть программного кода. Данный вывод основан на статистике Управления Организации Объединенных Наций по наркотикам и преступности. Так, согласно проведенному исследованию данной организации по 63 % уголовных дел, связанных с преступлениями в сфере информационных технологий, при создании вредоносных программ люди работали автономно и в большинстве случаев не было возможности установить всех лиц, причастных к процессу написания программного кода вредоносной программы[1].

После написания части программного кода вредоносной программы злоумышленники передают данный код лицам, которые используют его в преступных целях. В данном случае моментом создания вредоносного программного обеспечения будет момент «компиляции»[2] программы.

Стоит отметить, что вредоносная компьютерная программа имеет информацию о времени ее создания, однако оно прямо зависит от времени, установленного на ЭВМ, т. е. пользователь компьютера, который создает программное обеспечение, может его изменить.

В связи с этим для определения времени создания вредоносной компьютерной программы необходимо: во-первых, установить место, где она была создана; во-вторых, синхронизировать время, установленное на ЭВМ, с реальным временем; в-третьих,

---

[1] Всестороннее исследование проблемы киберпреступности : Управление Организации Объединенных Наций по наркотикам и преступности. URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/-UNODC_CCPCJ_EG4_2013_2_R.pdf.

[2] Компиляция – трансляция программы, составленной на исходном языке высокого уровня, в эквивалентную программу на низкоуровневом языке, близком машинному коду (абсолютный код, объектный модуль, иногда на язык ассемблера). Другими словами – процесс перевода из программного кода в программу, используемую ЭВМ (см.: Информационный портал «Уголовный кодекс РФ. URL: http://www. ruukrf.ru ; Компиляция // Информационный портал «Языки программирования». URL: http://programming-lang.com).

исследовать журнал операций по изменению времени на ЭВМ, которые производились пользователем.

Исходя из этого, по уголовным делам о преступлениях в сфере информационных технологий время совершения преступления должно пониматься в широком смысле и включать в себя:

1) время приискания лиц и средств для изготовления вредоносного программного обеспечения;

2) время создания вредоносного программного обеспечения (время написания программного кода и время компиляции, т. е. время фактического создания вредоносной программы);

3) время начала использования вредоносной программы;

4) время фактического использования указанной программы для получения выгоды.

При совершении преступлений в сфере информационных технологий злоумышленники часто уничтожают или изменяют компьютерные следы преступления (стирают или видоизменяют программный код с носителя информации). В таких случаях следователям следует руководствоваться последним установленным временем, так как в большинстве случаев данная информация не может быть восстановлена.

Другим способом сокрытия следов создания вредоносного программного обеспечения является размещение программного кода в открытых источниках, например в сети «Интернет». В этом случае временем изготовления вредоносного программного обеспечения следует считать момент получения данного вредоносного кода (момент скачивания на ЭВМ из сети «Интернет») и его компиляции.

2. **Место совершения преступления.** Понятие места совершения преступления на законодательном уровне не закреплено,

однако общепризнанно, что под местом совершения преступления следует понимать территорию, на которой совершается преступление[1].

Одной из особенностей преступлений в сфере информационных технологий следует считать их транснациональность (трансграничность). Трансграничность преступных деяний сильно усложняет установление фактического места совершения преступления, существенно затрудняет процесс раскрытия и расследования указанной категории уголовных дел.

Данный аспект в первую очередь обусловлен тем, что для совершения преступлений в сфере информационных технологий на территории одной страны необязательно фактическое присутствие в данной стране, чем пользуются злоумышленники в целях сокрытия следов преступления.

Кроме того, лица, совершающие преступления в сфере информационных технологий, используют различия в правовых системах государств, неодинаковый порядок уголовного преследования и т. д. Так, при написании программного кода вредоносной программы зачастую прибегают к помощи специалистов-программистов из тех стран, где данное деяние не является наказуемым, после чего с территории этих стран осуществляют «заражение» ЭВМ.

Надо отметить, что термин «территория» является условным понятием при расследовании уголовных дел о преступлениях в сфере информационных технологий. В глобальной сети «Интернет» чаще используется понятие сегментов[2]. Для определения тер-

---

[1] См., например: Российское уголовное право. Общая часть : учебник / под ред. Л. В. Иногамовой-Хегай, В. С. Комиссарова, А. И. Рарога. М., 2010. С. 42.

[2] Сегмент интернета – часть сайтов в глобальной сети «Интернет» с основным контентом (содержанием) на одном языке. Так, рунет – часть сайтов интернета с основным контентом на русском языке (см.: Руденков Н. А., Долинер Л. И. Основы сетевых технологий : учебник для вузов. Екатеринбург : Уральский федеральный ун-т, 2011).

ритории, где было совершено то или иное преступление, необходимо установить веб-сервер[1], на котором расположен конкретный сайт. Таким образом, с помощью веб-серверов и другого программного обеспечения преступления в сфере компьютерной информации могут быть начаты на территории одного государства, а продолжены и окончены – на территории других.

Исходя из вышеизложенного, понятие места совершения преступления в классическом виде не всегда применимо в полной мере при доказывании обстоятельств преступлений в сфере информационных технологий.

Правильное установление места совершения преступления имеет существенное значение не только для доказывания обстоятельств рассматриваемых преступлений, но и для определения территориальной подследственности.

По общему правилу уголовные дела расследуются по месту совершения преступления (ст. 152 УПК РФ). Это правило распространяется на все формы предварительного расследования.

При расследовании преступлений в сфере информационных технологий территориальная подследственность должна определяться территориальным нахождением организации (юридический адрес) кредитно-банковской сферы, на счет которой преступник перечислил похищенные денежные средства. Однако ни само лицо, совершившее преступление, ни потерпевший могут фактически не иметь к указанной территории никакого отношения.

Отмечая данную проблему, в июне 2014 г. Следственным департаментом МВД России в органы предварительного следствия направлены директивные указания (№ 17/3-16230 от 20 июня

[1] Сервер (от англ. to serve – служить) – специализированный компьютер и/или специализированное оборудование для выполнения на нем сервисного программного обеспечения (в том числе серверов тех или иных задач). Веб-сервер – специализированный компьютер для выполнения различных задач в глобальной сети «Интернет» (см.: Степанов А. Н. Информатика. 3-е изд. СПб. : Питер, 2002 ; Руденков Н. А., Долинер Л. И. Основы сетевых технологий).

2014 г.) об исключении необоснованного перенаправления в порядке ст. 152 УПК РФ материалов доследственной проверки о преступлениях рассматриваемой категории, влекущего увеличение сроков ее проведения и утрату следов преступления, необходимости при наличии достаточных оснований принимать процессуальное решение о возбуждении уголовного дела по месту поступления заявления о совершенном преступлении.

Кроме того, заместитель Генерального прокурора Российской Федерации В. Я. Гринь в информационном письме от 3 ноября 2015 г. № 36-11-2015 предлагает при осуществлении прокурорского надзора при передаче материалов проверок и уголовных дел учитывать следующую позицию: «…правомерным является признание территориальной подследственности в субъекте Российской Федерации, где непосредственно выполнялись действия, входящие в объективную сторону преступления, вне зависимости от того, что последствия наступили на другой территории, а также по месту наступления общественно опасных последствий…».

Исходя из вышеизложенного, под местом производства предварительного расследования следует понимать место фактического выявления признаков преступления.

Рассматривая вопрос о месте совершения преступления, нужно учитывать ранее обозначенное обстоятельство, что преступления в сфере информационных технологий включают в себя несколько этапов преступной деятельности, в связи с чем необходимо установить:

1) место или места написания программного кода вредоносной программы;

2) место компиляции указанной программы;

3) место нахождения объекта преступного посягательства.

При установлении места, где осуществлялось написание программного кода вредоносной программы, и места, где произ-

водилась компиляция данной программы, необходимо определить: во-первых, фактический адрес расположения ЭВМ, на которой осуществлялись указанные действия; во-вторых, место осуществления доступа к глобальной сети «Интернет»; в-третьих, место подключения к локальным сетям общего пользования или закрытым локальным сетям; в-четвертых, идентификационные номера компьютера (IP-адресов, MAC-адреса сетевого оборудования и др.).

Место нахождения объекта преступного посягательства устанавливается путем определения фактического места нахождения учреждения кредитно-финансовой сферы, со счета которой было совершено хищение (потерпевшего). При этом существенной особенностью является не только определение фактического места (адреса) организации, но и «доменного» адреса[1]. При установлении доменного адреса организации также устанавливается IP-адрес[2] и MAC-адрес[3] компьютера, который использовался для регистрации в сети «Интернет» и с которого были похищены денежные средства.

Таким образом, при установлении места совершения преступления необходимо устанавливать не только фактическое место нахождения организации, откуда были похищены денежные

---

[1] Доменный адрес или домен – символьное имя, служащее для идентификации областей – единиц административной автономии в сети «Интернет» – в составе вышестоящей по иерархии такой области. Другими словами – «адрес в глобальной сети «Интернет» (см.: Степанов А. Н. Информатика).

[2] IP-адрес – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP. Другими словами – «номер ЭВМ (сети ЭВМ), который присваивается поставщиком услуг, обеспечивающим доступ в глобальную сеть „Интернет”» (см.: Степанов А. Н. Информатика).

[3] MAC-адрес (от англ. Media Access Control – управление доступом к среде, также Hardware Address) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet. Другими словами – «уникальный номер элемента компьютера, обеспечивающего возможность подключения к сети, в том числе и к глобальной сети «Интернет», «аналог IMEI-адреса сотового телефона» (см.: Степанов А. Н. Информатика. СПб. : Питер, 2002).

средства, место нахождения ЭВМ, на которых был написан программный код вредоносной программы и на котором осуществлялась компиляция указанной программы, а также их электронный адрес, т. е. адрес в глобальной сети «Интернет».

При доказывании преступлений в сфере информационных технологий надо учитывать тот факт, что часто определить место совершения преступных деяний невозможно.

Примером данных случаев будут служить те факты, когда злоумышленники в своей преступной деятельности используют возможности сегмента глобальной сети «Интернет»: .ONION[1] или возможности интернет-ресурсов так называемого Дарк-Нета[2]. Данный сегмент интернета не имеет фактической привязки к физическим адресам, поэтому местом совершения преступления будет являться электронный (доменный) адрес в глобальной сети «Интернет».

---

[1] .Onion – псевдо-домен верхнего уровня (схожий по применению с доменами .bitnet и .uucp, использовавшимися ранее), созданный для обеспечения доступа к анонимным или псевдо-анонимным адресам сети Tor (сокр. от англ. The Onion Router). Подобные адреса не являются полноценными записями DNS, и информация о них не хранится в корневых серверах DNS, но при установке дополнительного программного обеспечения, необходимого для выхода в сеть Tor (например, Orbot для Android или плагин Torbutton для Firefox), программы, работающие с интернетом, получают доступ к сайтам в доменной зоне .onion, посылая запрос через сеть Tor-серверов (см.: Мониторинг Реестра запрещенных сайтов: статистика. URL: https://antizapret.info/index.php?search=onion.to ; Романова А. С. Борьба с преступностью в компьютерных сетях «глубинного» интернета : Материалы всероссийской научно-практической конференции «Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования». Иркутск, 2016. С. 122–127).

[2] ДаркНет – частная сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов (см.: TOR: a Dark Net Journey on How to Be Anonymous Online (TOR, Dark Net, DarkNet, Deep web, cyber security Book / John Smith. – North Charleston (SC) ; CreateSpace Independent Publishing Platform, 2017 ; Фролов А. А., Сильнов Д. С. Исследование механизмов рассмотрения запрещенного содержимого в DarkNet. Современные информационные технологии и ИТ-образование : «Лига интернет-медиа». 2017. № 4. С. 216–224.

Исходя из этого, можно сделать вывод, что местом совершения преступлений в сфере информационных технологий, в том числе против собственности, может являться как физический адрес нахождения объекта преступления, так и электронный адрес места нахождения ресурса, способствующему совершению преступления, который не имеет фактической привязки к физическому адресу, либо физический адрес указанного ресурса вообще невозможно установить.

3. **Способ совершения преступления.** Процесс доказывания способа совершения компьютерных преступлений – один из самых сложных, это обусловлено тем, что преступник постоянно пытается скрыть свои действия, а современные технические и технологические возможности и глобализация лишь способствует этому.

Исходя из гл. 28 УК РФ «Преступления в сфере компьютерной информации», по способам совершения компьютерных преступлений выделяют деяния, связанные: 1) с изъятием компьютерной информации; 2) с перехватом информации; 3) с несанкционированным доступом; 4) с манипуляцией информацией и ее подменой; 5) совершенные комплексными способами[1].

Однако к преступлениям в сфере компьютерной информации, связанных с хищением денежных средств, такая классификация является малоприменимой.

На первоначальном этапе расследования следователю известны лишь место фактического совершения преступного деяния, причиненный ущерб и личность потерпевшего. После установления данных фактов следующим вопросом, который будет требовать разрешения, является именно способ совершения преступления.

---

[1] Тер-Акопов А. А. Преступление и проблемы нефизической причинности в уголовном праве : монография. М. : Юркнига, 2003 ; Арзамасцев М. В. К вопросу об уголовно-правовой классификации киберпреступлений // Актуальные вопросы права и отраслевых наук. 2017. № 1 (3). С. 11–17.

Исходя из этого, следователь должен определить, каким способом было произведено «заражение» вредоносным программным обеспечением. И исходя из этого, складываются две основные следственные ситуации, обусловленные способами совершения преступления:

1. Вредоносным программным обеспечением заражена непосредственно ЭВМ, которая производила операции. Это могут быть ситуации, когда злоумышленники при помощи вредоносного программного обеспечения получали доступ к сервисам «онлайн Банка», к личным данным, позволяющим совершить хищение, и др.

2. Вредоносным программным обеспечением заражена ЭВМ, которая осуществляла обработку операции, – это те случаи, когда преступники «заражали» ЭВМ организаций, предоставляющие услуги населению в кредитной и банковской сфере[1].

Если установлено использование вредоносного программного обеспечения в совершении преступления, должны рассматриваться как минимум три основные версии способа совершения:

1. Физическое «заражение» ЭВМ (установка вредоносного программного обеспечения с различных переносных накопителей информации (карты памяти, «флеш-накопители информации», CD или DVD диски, цифровые устройства и др.).

2. «Заражение» ЭВМ из локальной сети (вредоносная программа может быть распространена через локальную сеть. Например, когда сотрудник организации использовал компьютер в личных целях, после чего подключился к рабочей сети и неведомо для себя распространил вредоносную программу).

3. «Заражение» ЭВМ из глобальной сети «Интернет». Это самый распространенный случай, способы его реализации могут

[1] Стоит отметить, что удельный вес преступлений второй группы на данный момент минимален, что во многом связано с тем, что данные учреждения тратят огромные ресурсы на обеспечение кибербезопасности.

быть различными и постоянно совершенствуются злоумышленниками. К ним можно отнести рассылку вредоносного программного обеспечения в социальных сетях или по электронной почте, создание дубликатов сайтов («фишинг») и др.

В процессе доказывания способа совершения указанных видов преступлений первоначально необходимо определить место нахождения вредоносного программного обеспечения в момент и время совершения хищения. Затем определить способы «заражения» вредоносным программным обеспечением. Далее необходимо установить источник, от которого произошла передача вредоносного программного обеспечения. При установлении данных фактов на заключительном этапе доказывания необходимо определить все пути распространения вредоносного программного обеспечения и установить «первоисточник». «Первоисточником» будет считаться ЭВМ, на которой было скомпилировано вредоносное программное обеспечение или на которой находилась его копия в момент начала реализации преступного умысла. Стоит отметить, что злоумышленники с целью сокрытия своего места нахождения часто пользуются программным обеспечением, которое изменяет или скрывает привязку к физическому адресу. Собирание доказательств, направленных на установление факта использования таких программ, имеет значение и для установления способа совершения преступления.

Таким образом, при определении способа совершения преступлений в сфере информационных технологий необходимо установить местонахождение вредоносного программного обеспечения в момент совершения хищения, способ «заражения», пути распространения от злоумышленника до потерпевшего.

Установление указанного в п. 2 ч. 1 ст. 73 УПК РФ обстоятельства, входящего в предмет доказывания по уголовным делам о преступлениях в сфере информационных технологий, – «виновность лица в совершении преступления» – неизбежно связано с установлением события данного преступления.

Примером может служить уголовное дело в отношении братьев Попелышей[1]. В ходе расследования данного уголовного дела было установлено время совершения преступления, а именно: время компиляции и начала использования вредоносного программного обеспечения – программы семейства Trojan.Win32.VKhost, время создания «фишинговых» сайтов, имитирующих страницы интернет-банкинга ВТБ 24 «Телебанк» и время фактического хищения денежных средств. Следователям удалось установить «место» (доменный адрес), где братья Попелыши привлекли к своей преступной деятельности Александра Сарбина, – сайт в сети «ДаркНета». Географическое положение места, где был вовлечен в преступную деятельность А. Сарбин и где размещались «фишинговые страницы банка», установить невозможно. Однако следователям с помощью экспертов удалось доказать полностью способ распространения вредоносного программного обеспечения.

Для того чтобы доказать виновность лица в совершении преступления в сфере информационных технологий, прежде всего, требуется установить место нахождения ЭВМ, которая использовалась в преступной деятельности. Однако установление данной вычислительной машины прямо не указывает на лицо, совершившее преступления. Для установления лица (лиц), совершивших указанные виды преступлений, зачастую необходимо произвести совокупность не только следственных действий и оперативно-разыскных мероприятий, но привлечь к участию в них лиц, обладающих специальными знаниями (экспертов, специалистов).

С помощью оперативных мероприятий следователь получает информацию о возможной причастности лица (лиц) к совершению указанного вида преступления, после чего путем проведения следственных и иных действий доказывает указанный факт.

---

[1] Дело о фишинге: как ловили хакеров-близнецов из Санкт-Петербурга // URL: https://ria.ru/incidents/20121221/915789715.html.

Однако в большинстве случаев в результате следственных действий будет установлено два основных факта: 1) лицо (лица) постоянно пользовались ЭВМ; 2) данная ЭВМ использовалась в преступной деятельности. Но этого недостаточно для предъявления обвинения.

В связи с этим в рамках предварительного расследования необходимо привлечение экспертов и специалистов, которые смогут установить факт применения (изготовления) вредоносного программного обеспечения конкретным лицом. Данные действия в каждом конкретном случае являются уникальными, так как деятельность преступников не строится «по одним шаблонам» и часто носит скрытый характер.

Исходя из этого, целесообразно привлечение специалиста при производстве первоначальных следственных действий и оперативно-разыскных мероприятий либо передача в распоряжение эксперта, производящего компьютерную экспертизу, не только всех материалов уголовного дела, но и всех изъятых предметов и документов. Данный факт будет способствовать идентификации личности преступника и сбору доказательств, подтверждающих его виновность.

Таким образом, в рамках общих правил досудебного производства по уголовным делам о преступлениях в сфере информационных технологий положения о предмете доказывания обладают существенной спецификой, что связано с особенностями установления времени, места и способа совершения указанных преступных деяний, а также виновности лиц, их совершивших.

§ 5.3. Деятельность следователя по осуществлению отдельных следственных действий при расследовании преступлений в сфере информационных технологий

В ходе проведения предварительного расследования, в том числе и по уголовным делам в сфере информационных технологий, следователь самостоятельно определяет перечень и порядок производства предусмотренных законом процессуальных действий.

Итак, приняв решение о возбуждении уголовного дела в порядке ст.ст. 144, 145 УПК РФ по факту совершенного преступления в сфере информационных технологий, следователь приступает к первоначальному этапу расследования, в ходе которого реализует задачи по выявлению и сбору доказательств, имеющих отношение к расследуемому уголовному делу.

Алгоритм деятельности следователя во многом зависит от сложившейся к данному времени следственной ситуации, с учетом которой им и планируется необходимый перечень следственных действий и оперативно-разыскных мероприятий. Анализ следственной практики свидетельствует о том, что планирование является важной составной частью деятельности следователя по расследованию преступлений в сфере информационных технологий, от полноты и качества которого зависит итоговый результат проведения конкретного следственного действия и расследования в целом.

Во время планирования необходимо максимально эффективно, с учетом минимальных затрат сил и средств в кратчайшие сроки выполнить комплекс следственных действий, позволяющих установить перечень обстоятельств, подлежащих доказыванию, предусмотренных в ст. 73 УПК РФ. Таким образом, достигается оптимизация процесса расследования, упорядочиваются следственные и иные процессуальные действия.

Характерной особенностью планирования следственных действий на первоначальном этапе расследования является недостаток у следователя сведений о произошедшем преступлении, динамически изменяющейся следственной ситуации, что в определенной степени связано со спецификой сферы информационных технологий.

Необходимо отметить, что значимым условием в эффективной деятельности следователя является реализация качественного взаимодействия во время осуществления следственных действий.

Осуществляемые после возбуждения уголовного дела первоначальные следственные действия (осмотр, допрос, обыск, выемка и другие) направлены на выявление и фиксацию информации, имеющей значение для расследования конкретного уголовного дела.

Одним из основных первоначальных следственных действий является **осмотр места происшествия**.

Под местом происшествия по делам о преступлениях в сфере информационных технологий необходимо понимать место, в пределах которого осуществлялись преступные действия, наступили вредные последствия, можно обнаружить следы преступления. К числу таких мест можно отнести:

– место обработки информации – предмета преступного посягательства (рабочее место, рабочая станция и т. д.);

– сервер, сохранивший свидетельства о работе системы за определенный период или о предмете посягательства;

– место использования технических средств для незаконных действий в сфере информационных технологий, создания, использования, распространения вредоносного ПО; непосредственного нарушения правил эксплуатации ЭВМ;

– место наступления вредных последствий, место хранения информации, полученной в результате неправомерного доступа, и др.

В ходе осуществления осмотра места происшествия, в зависимости от следственной ситуации, следователю в обязательном порядке необходимо прибегать к помощи специалиста в сфере информационных технологий, обладающего необходимыми навыками работы с современными техническими устройствами: специалисты по настройке, обслуживанию, ремонту компьютерной техники, сетевым технологиям, программисты, специалисты в области средств связи, информационно-телекоммуникационных систем и др. В каждом конкретном случае следователь должен определить, специалист какого рода необходим при производстве осмотра.

Следует отметить, что большую помощь в ходе данного следственного действия следователю также могут оказать оперативные сотрудники отдела «К» или других подразделений, а также участковый уполномоченный полиции, обслуживающий данную территорию, другие участники по мере необходимости.

Перед выездом на место происшествия особое внимание следователю необходимо обратить на подготовку в дополнение к традиционным криминалистическим средствам необходимых технических средств, которые могут пригодиться в предстоящем осмотре. К числу таких средств можно отнести: ноутбук, внешние жесткие диски, DVD и CD диски, набор соединительных кабелей, фото- и видеокамеры, программное обеспечение, упаковочные материалы и др.

В ходе осуществления осмотра по уголовным делам в сфере информационных технологий следователю помимо решения традиционных задач осмотра, связанных с установлением события преступления, времени, места, предмета, способа совершения преступления, необходимо особое внимание направить на обнаружение и работу со специфическими следами, характерными для указанных преступлений.

Перед началом осмотра места происшествия следователь должен обеспечить сохранность следов преступления, запретить

помимо привлекаемого к следственному действию специалиста доступ к компьютерной и иной вычислительной технике, электронным носителям информации, блокам электропитания и другому техническому оборудованию.

Никакое оборудование не должно включаться или выключаться без разрешения специалиста.

Приступая непосредственно к производству осмотра и составления протокола, необходимо обратить особое внимание:

– на наличие или отсутствие традиционных следов преступления: следы пальцев рук, обуви, следы повреждения, взлома, уничтожения и (или) модификации охранных и сигнальных устройств и др.;

– взаиморасположение, конструктивные и иные особенности обнаруженных технических устройств;

– наличие или отсутствие проводного и беспроводного соединения между обнаруженными техническими устройствами, наличие возможности выхода в сеть «Интернет»;

– наличие или отсутствие специальных технических средств, программного обеспечения для негласного получения (уничтожения, блокирования) компьютерной информации и оборудования.

В ходе осмотра и описания технических устройств, обнаруженных на месте происшествия, необходимо обращать внимание на общие (вид, название, модель и другие) и частные индивидуальные признаки (заводской, инвентарный номер и другие), а также, каким способом, при помощи чего, с какими внешними устройствами они связаны.

В случаях если на момент осмотра технические устройства находятся в рабочем включенном состоянии, следователю необходимо это отразить в протоколе осмотра с указанием информации, выведенной на табло (экран). В случае если обнаруженные

технические устройства на момент осмотра находились в выключенном состоянии, то необходимо чтобы решение о целесообразности его включения принимал специалист.

Настоятельно рекомендуется фиксировать в протоколе осмотра содержание и последовательность действий специалиста с осматриваемым техническим оборудованием, программным обеспечением и другими не менее важными обнаруженными на месте объектами.

Также необходимо обратить внимание на записные книжки, тетради и иные объекты, в которых может содержаться интересующая следователя информация о логинах, паролях, телефонах, физических или юридических лицах и иная способствующая расследованию информация.

Подробный осмотр обнаруженных технических устройств, электронных носителей информации, иного оборудования производится в ходе осмотра места происшествия либо последующего самостоятельного следственного действия с учетом конкретной сложившейся ситуации.

Отражать в протоколе сведения об обнаруженных технических устройствах рекомендуется от общих к индивидуальным признакам.

Флеш-накопители встречаются в виде флеш-дисков и флеш-карт. Необходимо описать внешний вид, тип, маркировку и другие особенности осматриваемого объекта.

Описывая CD, DVD, Blu-ray диски, указывают: тип, маркировку, количество предназначенных для записи информации рабочих сторон, наличие надписей, цифровых и иных индивидуальных особенностей.

Осуществляя осмотр информации на электронном носителе, в протоколе следственного действия необходимо отражать всю пошаговую последовательность производимых манипуляций с указанием технических устройств и программного обеспечения для этого задействованных.

При осмотре файлов отражаются его наименование, тип, дата создания, изменения, объем информации, сведения об авторе и другие индивидуальные атрибуты.

В ходе осмотра страниц сайтов в протоколе необходимо отразить сведения о применяемых технических устройствах (ПК, принтер и др.), операционной системе (Windows, Mac OS, Unix и др.), браузере (Internet Explorer, Google Chrome, Yandex Browser и др.), данные о провайдере, предоставившим доступ в сеть «Интернет». Затем описывается пошаговый доступ к страницам интернет-сайта с указанием всех ссылок, к которым следователь должен будет обратиться для осмотра информационного ресурса; электронные адреса страниц; осматривается собственно содержание страницы; указывается, находится ли информация в свободном доступе или требуется регистрация. К протоколу приобщается твердая копия скриншота страницы сайта.

При осмотре обнаруженных мобильных телефонов указывают наличие или отсутствие SIM-карты, ее номер и оператора; IMEI (указан на телефоне под аккумулятором; можно также для получения IMEI набрать на клавиатуре телефона комбинацию *#06# и нажать кнопку вызова), после описания внешних признаков целесообразно изучить папки «сообщения», «контакты», «вызовы», «изображения», «видео». Контакты могут указываться с формулировкой: «…имеется 134 контакта, абонентские номера с привязкой к именам:…», при осмотре сообщений приводится текст сообщения, от кого, дата поступления.

Решение о необходимости изъятия обнаруженного технического оборудования, информации и иных следов следователь принимает с учетом сложившейся следственной ситуации и требований закона.

В ст. 82 УПК РФ законодателем предусмотрена возможность после производства неотложных следственных действий в случае невозможности возврата изъятых в ходе производства следственных действий электронных носителей информации их

законному владельцу копирования содержащейся на этих носителях информации. Копирование указанной информации происходит на другие электронные носители информации, предоставленные законным владельцем изъятых электронных носителей информации или обладателем содержащейся на них информации, и осуществляется с участием законного владельца изъятых электронных носителей информации или обладателя содержащейся на них информации и (или) их представителей и специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде. При копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения. Не допускается копирование информации, если это может воспрепятствовать расследованию преступления. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации составляется протокол.

Изъятое оборудование перевозится в выключенном состоянии.

Необходимо учитывать, что на компьютере может быть установлено вредоносное программное обеспечение, которое может при неквалифицированном обращении повредить интересующую следователя информацию, а также само техническое устройство.

В ходе **осмотра** ранее **изъятых предметов и документов**, в том числе видеозаписей по уголовным делам в сфере информационных технологий, необходимо уделить внимание следующим особенностям:

– номерам банковских карт, банковских счетов, абонентских номеров, с которых или на которые перечислялись похищенные денежные средства;

– адресам расположения базовых станций и векторов (азимутов) направления сигнала;

– IP-адресам, с которых осуществлялись неправомерный доступ к банковскому счету, создание и администрирование учетной записи (аккаунта в социальных сетях, электронного почтового ящика, электронного кошелька и пр.), доступа к личному кабинету интернет-ресурса;

– MAC-адресам сетевых карт (встроенных сетевых интерфейсов) компьютерной техники, а также Wi-Fi-роутеров;

– номерам объявлений на специализированных сайтах объявлений (досках объявлений);

– чертам внешности, поведения, одежде подозреваемого лица, а также детально о производимых им действиях (манипуляциях) с указанием точного времени их осуществления.

При осуществлении осмотра электронных носителей информации рекомендуется привлечь к участию специалиста.

Специалистом (в присутствии понятых) производится подключение своего ноутбука к сети или ЭВМ пострадавшего для проведения антивирусного тестирования системы.

Осуществив указанное подключение, специалист проводит тестирование персональных компьютеров и сети на предмет обнаружения вредоносных (либо пораженных вирусом) программ. Для их обнаружения используется соответствующее антивирусное и вирусодетектирующее программное обеспечение.

С целью получения образцов для последующего сравнительного исследования (файлов), успешного проведения данного и последующих действий и недопущения нанесения вреда системе необходимо произвести полное резервное копирование файлов сетевой среды на внешние носители информации либо на ноутбук специалиста.

Полная копия данных в дальнейшем изымается для приобщения к уголовному делу и детального исследования в качестве ве-

щественного доказательства. Следователем истребуются предыдущие резервные копии (если таковые существовали) для последующего экспертного исследования в лабораторных условиях. Затем проводится антивирусное тестирование. Специалист должен учитывать, что определенные в результате тестирования зараженные файлы не должны «вылечиваться». Факты обнаружения вредоносных программ только фиксируются, а зараженные файлы в дальнейшем будут переданы эксперту для дальнейшего исследования с целью установления групповой принадлежности обнаруженных вирусов, их распространенности в сетевых средах других организаций, вредоносных последствий их использования, оценки даты их написания и степени квалификации лица, создавшего и (или) внедрившего данный программный код.

Значимая компьютерная информация также может быть обнаружена не только следователем при производстве следственного действия, но и экспертом при проведении экспертного исследования ЭВМ, системы ЭВМ, их сети и машинных носителей.

Расследование преступлений в сфере информационных технологий сопряжено с необходимостью использования специальных знаний, терминологии, которыми не всегда обладают следователи. Чтобы устранить данные сложности, следователю рекомендуется помимо принятия решения о привлечении к участию в следственном действии специалиста предварительно и самому у него проконсультироваться по основным вопросам предстоящего **допроса**, а также: проанализировать материалы дела, определить последовательность необходимых допросов, изучить личность допрашиваемого, выбрать тактику допроса, подготовить план допроса.

В ходе допроса можно столкнуться со специальными терминами, жаргонными понятиями. Посредством постановки уточняющих вопросов следователю необходимо постараться раскрыть их содержание.

Обязательному выяснению подлежат обстоятельства, указанные в ст. 73 УПК РФ.

В ходе допроса потерпевших можно выявить обстоятельства выявления преступления и его последствия, предварительно оценить причиненный ущерб, узнать способы защиты информации, порядок организации охраны объекта, точные данные о предмете преступного посягательства, предварительные данные о личности виновного и ряд других обстоятельств.

Начинать допросы свидетелей либо потерпевших целесообразно с лиц, которые обнаружили факт совершения преступления или его последствия.

К числу типовых вопросов можно отнести следующие[1]:

– при каких обстоятельствах были обнаружены следы преступления в сфере информационных технологий, в том числе следы работы вредоносного программного обеспечения (невозможность доступа к информационным ресурсам, изменение учетных данных, размещение сторонним лицом информации ограниченного доступа и т. п.);

– какие события предшествовали совершению преступления. При разрешении данного вопроса важно установить круг лиц, состоящих в близких, семейных либо рабочих отношениях, которые могли иметь возможность доступа к учетным данным пользователя, в том числе к его мобильному телефону. Поступали ли потерпевшему в предшествующий период SMS-сообщения или электронные письма с указанием интернет-ссылок от неизвестного источника, не было ли сбоев в работе учетных записей в социальных сетях, сообщались ли учетные данные кому-либо;

– предпринимались ли им после этого какие-либо самостоятельные действия по установлению события преступления;

[1] Преступления в сфере компьютерной информации: квалификация и доказывание : учебное пособие / под ред. Ю. В. Гаврилина. М., 2003. С. 136.

– имеются ли у него документы, подтверждающие факт неправомерного доступа (в том числе скриншоты), претензионные требования в адрес администрации интернет-ресурсов;

– имеются ли документы, подтверждающие факт общения потерпевшего с лицом, совершившим неправомерный доступ (например, если последний в результате неправомерного доступа получил сведения конфиденциального характера и требует выкуп за их неразглашение);

– причинен ли в результате неправомерного доступа материальный ущерб; какова точная сумма причиненного преступлением ущерба. (При решении вопроса о значительности причиненного вреда необходимо исходить из имущественного положения физического лица, выяснив размер его личных доходов, доходов семьи, наличие иждивенцев, кредитных или иных имущественных обязательств и другие вопросы.)

В ходе допроса подозреваемого (обвиняемого) следователю помимо стандартных вопросов также необходимо выяснить:

– наличие навыков программирования либо иных по владению электронно-вычислительной техникой;

– для какой цели осуществлялся неправомерный доступ к охраняемой законом информации (корыстные побуждения, ревность, шантаж и пр.);

– каким способом осуществлялся доступ к сети «Интернет». С использованием какой электронно-вычислительной техники, прямым подключением через кабель, с использованием Wi-Fi, флеш-модема, мобильного интернета и т. д.;

– наименование сетевого ресурса, используемого для совершения преступления;

– где и при каких обстоятельствах были оформлены интересующие следствие SIM-карты, банковские карты, оформлены банковские счета. Какие документы при этом предоставлялись;

– при каких обстоятельствах был создан интернет-сайт либо учетная запись в сервисах электронной почты, электронных

платежных системах, социальных сетях, мессенджерах. Каким образом осуществлялось администрирование указанных ресурсов, какой контент на них размещался;

– при каких обстоятельствах была создана или получена вредоносная программа. Посредством каких электронных ресурсов распространялась;

– что известно о принципах работы и функциональном назначении программного обеспечения либо конкретного программного продукта, имеется ли он в свободном доступе, требует ли регистрации на сайте производителя;

– совершались ли ранее аналогичные деяния;

– какие банкоматы либо устройства самообслуживания использовались для осуществления преступной деятельности с указанием адреса и месторасположения.

Дополнительные вопросы задаются по мере необходимости.

Спланированный и своевременно проведенный **обыск (выемка)** является одним из наиболее эффективных инструментов в арсенале следователя, позволяющий получить важные для следствия доказательства в ходе расследования преступлений в сфере информационных технологий.

Итак, в процессе подготовки к обыску (выемки) в помещениях следователю необходимо:

– провести тщательное планирование предстоящего следственного действия;

– провести анализ информации о месте проведения, собственнике, иных проживающих лицах. При необходимости дополнительную информацию можно запросить в подразделении миграции, выписку из домовой книги, справку из домоуправляющей компании, справку от участкового уполномоченного, справку из БТИ или Росреестра, сведения от судебных приставов (о возможных наложенных исполнительных мерах);

– провести предварительные консультации со специалистами в сфере информационных технологий, подготовить необходимые технические устройства для обработки, считывания и хранения изъятой информации, упаковочный материал;

– определить состав участников данного следственного действия (целесообразно пригласить как минимум специалиста и оперативных работников);

– заблаговременно осуществить оперативное совещание-инструктаж с сотрудниками оперативных подразделений, определив тактику его проведения.

Реализуя фактор внезапности и постаравшись максимально быстро войти в обыскиваемое помещение, не дав отключить, повредить либо иным образом негативно воздействовать на интересующую следователя информацию, оборудование, необходимо предложить лицу произвести его добровольную выдачу.

Кроме того, необходимо предложить добровольно выдать предметы, запрещенные к свободному гражданскому обороту, деньги и ценности, добытые преступным путем, а также компьютер и носители информации, использовавшиеся для преступных целей. Если происходит добровольная выдача ЭВМ и (или) электронных носителей информации, необходимо акцентировать внимание понятых на этом факте и уточнить у виновного, с какими именно преступными целями использовалась аппаратура, о чем сделать соответствующую запись в протокол.

Компьютер по согласованию со специалистом можно включить, записать его характеристики, операционную систему, имеется ли пароль при входе в систему, описать вид рабочего стола компьютера и вынесенные на него иконки запускаемых приложений, а также другие данные, о которых подробно рассказывалось при рассмотрении вопроса о производстве осмотра. Целесообразно привлечь виновного к даче пояснений в процессе осмотра ЭВМ и носителей информации.

По делам о преступлениях в сфере информационных технологий при обыске и выемке изыматься могут различные предметы и документы. Кроме этого могут изыматься: средства электросвязи, специально разработанные и приспособленные технические устройства (например, скиминговое оборудование), «реальный пластик» (т. е. поддельные полноценные твердые копии банковских карт), «белый пластик», (т. е. карты, имеющие только записанную магнитную полосу); вредоносное ПО, всевозможные документы (в том числе и электронные), отражающие и регламентирующие различные операции, технологические процессы, связанные с обработкой, накоплением, созданием, передачей и защитой компьютерной информации.

Следует обращать внимание и на традиционные источники доказательственной информации – специальную литературу (рекламные проспекты, справочники и каталоги по компьютерной технике, пособия и учебники по обработке, защите, передаче и негласному получению компьютерной информации), распечатки компьютерной информации, документы о соответствующем профессиональном образовании, свободные образцы почерка, документы, черновики и иные записи, которые можно использовать в последующем для сравнительного исследования.

Особое внимание рекомендуется обращать на записи паролей, логинов, электронных адресов, алгоритмы входа и работы в компьютерных системах и сетях.

К проведению обыска рекомендуется привлекать сотрудников ЭКЦ, специализирующихся на производстве компьютерных экспертиз. В исключительных случаях привлекать к участию в обысках следует иных лиц, имеющих основное или дополнительное образование в сфере информационных технологий. Таковыми могут являться:

– сотрудники оперативных подразделений (отдела «К» БСТМ субъекта Российской Федерации), но тогда необходимо

будет исключить возможность их дальнейшего участия в производстве оперативно-разыскных мероприятий и отдельных следственных действий;

– сотрудники, которые по роду своей деятельности непосредственно связаны со сферой информационных технологий (например, сотрудники отделов, обеспечивающих образовательный процесс в образовательных организациях МВД России, и т. д.);

– специалисты сторонних организаций, которые также по роду своей деятельности непосредственно связаны со сферой информационных технологий.

Принимая во внимание стрессовое состояние лиц, у которых проводится обыск, необходимо принять меры по добровольному получению от них паролей доступа к ресурсам электронно-вычислительной техники.

В ходе обыска обязательному изъятию по необходимости либо по результатам консультации со специалистом подлежат следующие предметы и документы:

– все виды электронно-вычислительной техники, так как искомая информация может храниться в цифровом виде на носителях, содержащихся в персональных компьютерах, ноутбуках, нетбуках, планшетных компьютерах, MP3-плеерах, диктофонах, цифровых фотоаппаратах, смартфонах, автомобильных регистраторах, системах видеорегистрации и т. д. Обратить внимание, что устройства, оснащенные автономным питанием, для исключения возможности их несанкционированного включения целесообразно упаковывать в коробки, так как пакеты этому не препятствуют. При изъятии, упаковке и транспортировке избегать взаимодействия с магнитными полями, в том числе с магнитосодержащими средствами криминалистической техники (например, магнитными кисточками);

– все типы энергонезависимых носителей информации (НЖМД-накопители на жестких магнитных дисках, флеш-накопители, zip-накопители, дискеты и пр.);

– носители однократной и многократной записи (оптические диски CD-R, DVD-R, CD-RW, DVD-RW, Blu-ray);

– сетевые устройства различных видов (сетевые карты, концентраторы, коммутаторы, маршрутизаторы, беспроводные сетевые адаптеры, точки беспроводного доступа и пр.). Кроме того, в обязательном порядке с целью избегания необходимости повторного проведения обыска необходимо установить наличие и изъять сетевое оборудование беспроводного доступа (Wi-Fi роутер), так как при последующем исследовании протоколов работы (log-файлов) в сети будет указан MAC-адрес беспроводного сетевого оборудования;

– средства мобильной связи, SIM-карты, базы от SIM-карт (пластиковая рамка, из которой извлекается SIM-карта перед установкой), договоры на подключение услуг подвижной и стационарной радиочастотной связи. Примечательно, что, как правило, при производстве обысков базы от SIM-карт не изымаются, хотя на них содержится ICCID – уникальный серийный номер SIM-карты, по которому можно идентифицировать абонентский номер SIM-карты. При имеющейся возможности средства мобильной связи перевести в авиарежим для исключения возможности их удаленного блокирования;

– средства криптографической защиты информации (аппаратные, программные, программно-аппаратные);

– иные предметы и документы, имеющие значение для доказывания.

В случае обнаружения наличия на включенных компьютерах криптоконтейнеров и доступа к облачным хранилищам рекомендуется перед их отключением и упаковкой осмотреть и скопировать информацию с компьютеров.

Выемка осуществляется следователем во многом по схожим с обыском правилам, но имеет свои отличительные особенности.

Значительную помощь в расследовании указанных преступлений следователю может оказать потерпевший. В ходе допроса он

может пояснить важную информацию, в том числе о предметах, документах и иной, имеющей значение для дела, которую следователь может получить посредством осуществления выемки.

Можно произвести выемку: документов, кассовых чеков, технических устройств и другие сведения. В случае если интересующая информация находится в памяти электронно-вычислительной техники потерпевшего, произвести ее выемку, осмотр с участием потерпевшего и специалиста (при необходимости), после чего вынести постановление о признании и приобщении изъятого к материалам уголовного дела в качестве вещественных доказательств. При наличии возможности вынести постановление о возвращении изъятого имущества потерпевшему.

В учреждениях связи, предоставляющих услуги по доступу к сети «Интернет», следователь в ходе выемки может получить сведения:

– об абоненте с указанием его установочных данных;

– номере и дате заключенного договора об оказании телематических услуг с приложением заверенной копии договора;

– протоколах работы в сети «Интернет» (log-файлы);

– IP-адресах, с которых осуществлялись создание и администрирование аккаунта;

– абонентах, которым в указанный момент времени выдавался установленный IP-адрес;

– MAC-адресах как самой компьютерной техники, так и сетевого оборудования, с использованием которых осуществлялся доступ к сети «Интернет».

Кроме того, при установлении факта наличия видеозаписи в местах расположения компьютерного оборудования, при помощи которого было совершено преступление (компьютерные клубы, устройства самообслуживания, интерактивные информационные панели и т. п.), либо места свободного доступа к открытой сети Wi-Fi (помещения торговых центров, мест общепита, транспорта и пр.) необходимо произвести ее изъятие в ходе выемки.

Наложение ареста на имущество не является следственным действием, при этом необходимо рассмотреть некоторые вопросы, связанные с данной процессуальной деятельностью следователя, в целях последующего возмещения имущественного вреда, причиненного преступлением в сфере информационных технологий.

В соответствии с п. 3.1 ч. 2 ст. 82 УПК РФ деньги, ценности и иное имущество, полученные в результате совершения преступления, а также доходы от этого имущества, обнаруженные при производстве следственных действий, подлежат аресту в порядке, установленном ст. 115 УПК РФ.

Арест может быть наложен на деньги, ценности и иное имущество, которое получено в результате совершения хотя бы одного из преступлений, предусмотренных статьями, указанными в п. «а» ч. 1 ст. 104.1 УК РФ, если доходы от этого имущества были частично или полностью превращены или преобразованы. Кроме того, арест можно наложить на оборудование или иные средства совершения преступления, принадлежащие подозреваемому (обвиняемому).

Примером могут послужить материалы уголовного дела, расследованного следственной частью СУ УВД по ЦАО ГУ МВД России по г. Москве по ч. 3 ст. 159.6 УК РФ. Было установлено, что неизвестные лица в период с 15 по 16 апреля 2014 г., используя компьютерную технику, при не установленных следствием обстоятельствах получили неправомерный доступ к торговым счетам И., открытым в ЗАО «XXXX», тем самым получив возможность полного распоряжения и управления находящимися на них контрактами и денежными средствами. Далее указанные не установленные следствием лица в целях хищения имущества И. совершили от его имени, но в своих интересах заведомо невыгодные сделки купли/продажи контрактов на фондовой бирже ММВБ, в результате чего денежные средства со счетов И. в размере свыше 1,5 тыс. руб. были перечислены на

подконтрольный им торговый счет, открытый в ООО «ХХХХХХ» на имя С. На денежные средства, находящиеся на брокерском счете С., открытом в ООО «ХХХХХХ», был наложен арест.

В случаях если имущество, полученное в результате совершения преступления, и (или) доходы от этого имущества были приобщены к имуществу, приобретенному законным путем, конфискации подлежит та часть этого имущества, которая соответствует стоимости приобщенного имущества и доходов от него.

Необходимо учитывать, что не на все имущество можно наложить арест.

Так, в соответствии с ч. 4 ст. 115 УПК РФ арест не может быть наложен на имущество, на которое в соответствии с гражданско-процессуальным законодательством не может быть обращено взыскание в соответствии со ст. 446 ГПК РФ.

Несмотря на то что имеются противоположные мнения относительно взаимосвязи таких процессуальных действий, как заявление гражданского иска и возможности наложения ареста на имущество, следователю в целях повышения эффективности данной меры необходимо в досудебном производстве, в наиболее сжатые сроки после возбуждения уголовного дела и установления искомого имущества решить данный процессуальный вопрос.

При этом следователь, принимая решение о наложении ареста на имущество, всегда должен четко осознавать, что данная мера процессуального принуждения призвана предупреждать сокрытие, дарение, переоформление на третьих лиц, распродажу или иное отчуждение имущество подозреваемого (обвиняемого) или лиц, несущих по закону материальную ответственность за действия последних.

Следователю необходимо достоверно установить принадлежность имущества подозреваемому (обвиняемому), иным лицам, которые несут материальную ответственность за действия

указанных субъектов, либо преступное происхождение имущества посредством осуществления комплекса следственных и иных процессуальных действий, а также оперативно-разыскных мероприятий.

Необходимую информацию об имуществе, на которое может быть наложен арест, следователь может получить:

– из Федеральной службы государственной регистрации кадастра и картографии (Росреестр)[1] и отделений Бюро технической инвентаризации (БТИ);

– Федеральной налоговой службы (ФНС России)[2];

– Государственной инспекции безопасности дорожного движения МВД России;

– Государственной инспекции маломерных судов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий[3];

– банков и иных кредитных организаций[4];

---

[1] Постановление Правительства Российской Федерации от 1 июня 2009 г. № 457 «О Федеральной службе государственной регистрации, кадастра и картографии» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_88583/.

[2] Постановление Правительства Российской Федерации от 30 сентября 2004 г. № 506 «Об утверждении Положения о Федеральной налоговой службе» // Российская газета. 2004. № 219.

[3] Постановление Правительства Российской Федерации от 23 декабря 2004 г. № 835 «Об утверждении Положения о Государственной инспекции по маломерным судам Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_-50876/. Режим доступа: по расписанию.

[4] Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/-document/cons_doc_LAW_5842/.

– Национального центрального бюро Интерпола[1].

Своевременно полученная из указанных государственных органов информация позволит следователю организовать незамедлительное проведение следственных действий, направленных на выявление имущества и денежных средств, подлежащих аресту, в целях последующего удовлетворения требований гражданских истцов по уголовным делам.

Использование современных информационных баз данных (страховых компаний, бюро кредитных историй и т. п.), а также сведений, содержащихся в аккаунтах подозреваемых (обвиняемых) социальных сетей («Одноклассники», «ВКонтакте», «Фейсбук» и др.), также могут оказать содействие следователю в установлении имущества, на которое может быть наложен арест.

В случаях же хищения денежных средств с расчетных счетов физических и юридических лиц целесообразно осуществлять розыск похищенных денежных средств путем истребования в банках выписок по расчетным счетам, с последующим обращением в суд с ходатайством о наложении ареста на денежные средства в целях недопущения их последующего перевода, обналичивания.

Наложение ареста на имущество является одним из процессуальных элементов деятельности следователя, осуществляемого с учетом проведенного комплекса следственных и иных процессуальных действий, а также оперативно-разыскных мероприятий, позволяющих пресечь действия подозреваемого (обвиняемого) по сокрытию, отчуждению денежных средств и иного имущества, и обеспечить возмещение вреда причиненного преступлением, в том числе и в сфере информационных технологий.

---

[1] Приказ МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971 от 6 октября 2006 г. «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_63834/. Режим доступа: по расписанию.

ГЛАВА 6. Использование специальных знаний при расследовании преступлений в сфере информационных технологий

§ 6.1. Поиск компьютерной информации. Сбор данных с устройств на базе ОС MS Windows

Прежде чем приступить к раскрытию содержания данного параграфа, необходимо сделать некоторое отступление в целях формирования правильного понимания сути работы с компьютерной информацией и возможностей ее исследования.

Известно, что применение специальных знаний осуществляется в процессуальной и непроцессуальной формах, следовательно, существуют различия в получении информации с компьютерных средств и вытекающие из них особенности применения соответствующих методов. При этом необходимо отметить, что вне зависимости от применяемых средств главенствующим принципом работы с компьютерной информацией является обеспечение ее неизменности и сохранности, о чем будет сказано ниже. Безусловно, имеют место обстоятельства, когда при реализации процессуальной формы данное правило вынужденно нарушается, однако это должно происходить исключительно по разрешению лица, назначившего экспертизу или проводящего следственное действие. В непроцессуальной же форме (проведение оперативных мероприятий, предварительных исследований) такие шаги недопустимы, так как могут поставить под угрозу формирование доказательственной базы, если информация будет подвержена изменению в ходе ее обнаружения, изъятия и исследования. Следует помнить, что любые, даже самые незначительные манипуляции с включенным компьютером влекут изменение данных на его носителе информации. Например, при загрузке ОС уже происходит изменение системных файлов (об-

новление записей в реестре, системных журналах и др.), при подключении USB-накопителя к работающему компьютеру происходят запись системных файлов на накопитель и изменение информации в реестре ОС. Поэтому в целях соблюдения вышеуказанного принципа исследуемое компьютерное средство (стационарный компьютер, ноутбук, сервер) экспертом не включается, а для исследования данных из него извлекаются носители информации. То же самое происходит и при осмотре компьютера или носителя информации с участием специалиста, для чего последний должен иметь набор оборудования и программного обеспечения для работы в мобильных условиях.

Также сотрудникам, участвующим в процессе раскрытия и расследования преступлений в компьютерной сфере, необходимо четко понимать, что любая обнаруженная информация, с какой бы очевидностью она ни указывала на конкретное лицо или обстоятельства, – это, по сути, обезличенный набор данных, происхождение и принадлежность которых еще предстоит установить в ходе экспертизы и иных следственных действий.

Действия при осмотре компьютера на базе ОС Windows

Рассмотрим варианты осмотра работающего компьютера и выключенного компьютера или носителя информации. В обоих случаях наиболее предпочтительный путь – это получение образа накопителя и дальнейшая работа с ним.

Однако при осмотре работающего компьютера важно зафиксировать так называемые короткоживущие данные, которые могут иметь значение для дела. Это перечень выполняемых в системе прикладных программ и процессов, временные файлы, содержимое оперативной памяти и файла подкачки. Существует достаточно много утилит, предоставляющих возможности для сохранения таких данных, однако следует помнить, что запуск и тем более установка какой-либо программы (тем более имеющей графический интерфейс) влекут за собой изменения данных

на носителе информации, поэтому необходимо минимизировать любые манипуляции в программной среде осматриваемой системы.

Именно поэтому нижеописанные действия с работающим компьютером допускается проводить только в случаях, когда прерывание его работы и изъятие невозможны. В остальных случаях рекомендуется выключить компьютер, изъять накопитель, снять копию данных имеющимися в распоряжении специалиста средствами.

Итак, при осмотре **работающего** компьютера в первую очередь необходимо получить максимально «чистые» от постороннего вмешательства образы оперативной памяти и носителя информации.

Получение снимка оперативной памяти

Снимок оперативной памяти создается с помощью специальных утилит, например FTK Imager. Порядок действий:

1. Программный продукт FTK Imager предварительно записывается на сменный USB-носитель.

2. Сменный носитель, содержащий FTK Imager, необходимо подключить к ЭВМ, образ НЖМД которой требуется скопировать.

3. Далее подключается сменный носитель информации, на который будет скопирован образ. **ВНИМАНИЕ!** Наиболее предпочтительным является вариант использования **одного** внешнего накопителя с объемом, достаточным для хранения как инструментария специалиста, так и создаваемых образов. Это могут быть внешние USB-накопители объемом от 1 Тб, а также аналогичного или большего объема НЖМД с интерфейсом SATA, подключаемые посредством адаптера SATA – USB.

4. Запускается файл «FTK Imager.exe» с правами администратора.

После загрузки появляется главное окно (рис. 6.1).

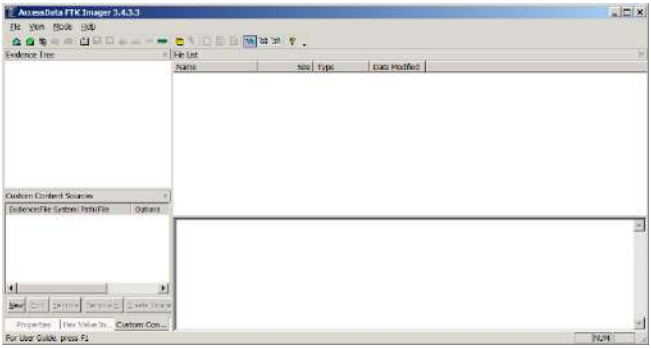


Рис. 6.1. Главное окно FTK Imager

Выбирается пункт меню File – Capture Memory (рис. 6.2).

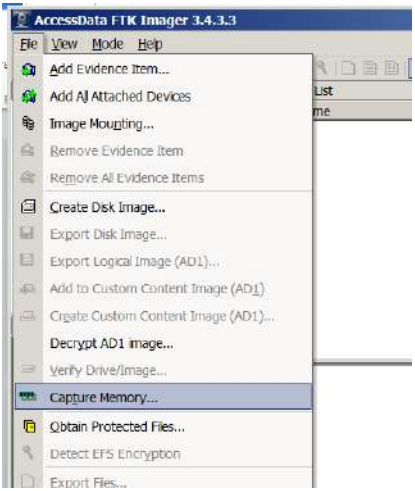


Рис. 6.2. Снимок оперативной памяти

Необходимо указать целевое устройство, на которое будет сохранен снимок, путем нажатия кнопки Browse (рис. 6.3).

Также необходимо отметить галками Include pagefile и Create AD1 file. После этого необходимо нажать кнопку Capture Memory. В результате в выходной папке окажутся необходимые снимки.

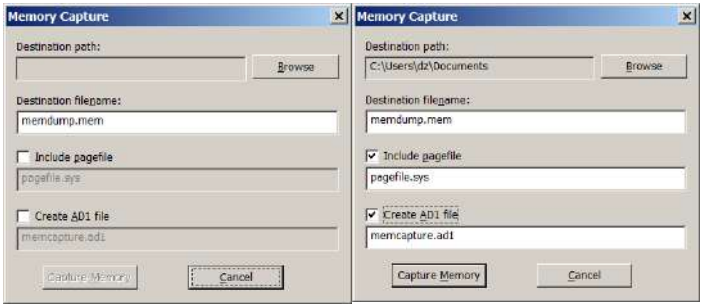


Рис. 6.3. Настройки снимка

Получение копии данных с накопителя (НЖМД)

Следует помнить, что традиционное копирование методом copy-and-paste не является полным, так как им не охватываются, во-первых, скрытые данные, среди которых могут быть как системные, так и пользовательские; во-вторых, условно свободные области накопителя, содержащие удаленные пользователем данные, которые также не будут скопированы. Поэтому копирование данных производится путем создания точного образа содержимого накопителя с помощью той же утилиты FTK Imager.

Первоначальный порядок действий схож со снятием снимка оперативной памяти. После загрузки программы появляется главное окно.

Выбирается пункт меню File – Create Disk Image. Будет отображено окно выбора типа источника данных (рис. 6.4).

В качестве типа источника чаще всего используется «Физический диск». Выбор «Логический диск» рекомендуется в следующих случаях:

– носители информации в ЭВМ образуют программный отказоустойчивый массив (RAID), а данные следует скопировать в декодированном виде (для исключения проблем с дальнейшей сборкой массива);

– используется программное шифрование всего содержимого носителей информации в ЭВМ (полнодисковое шифрование), а данные следует скопировать в расшифрованном виде.

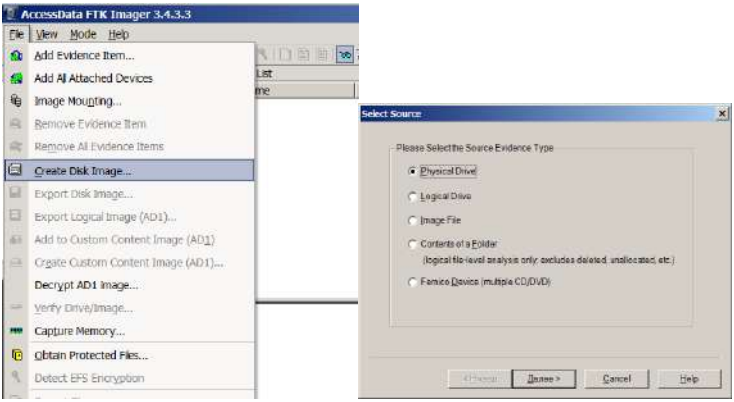


Рис. 6.4. Создание образа

Далее необходимо выбрать источник данных (рис. 6.5).

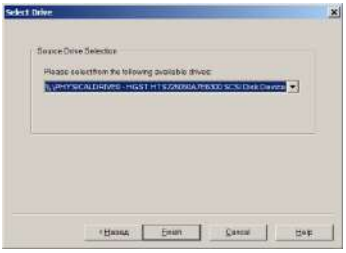


Рис. 6.5. Устройство – источник

Отображается общее окно параметров создаваемых образов. В указанном окне следует нажать кнопку Add (рис. 6.6).

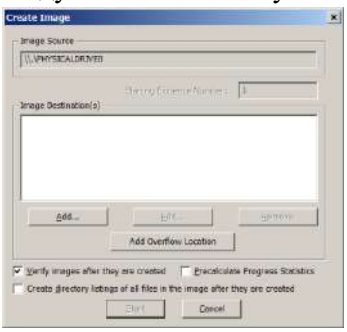


Рис. 6.6. Создание образа

Отображается окно выбора типа создаваемого образа. В указанном окне рекомендуется выбрать Raw (dd) (точная копия данных без сжатия или шифрования) (рис. 6.7).

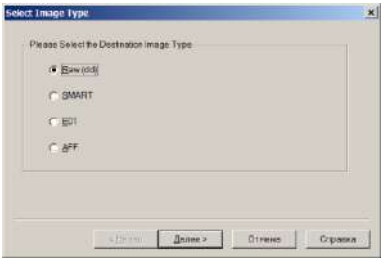


Рис. 6.7. Выбор типа образа

Окно ввода дополнительной информации не является обязательным к заполнению. Рекомендуется ввести фамилию человека, создающего образ (поле Examiner), и сведения, указывающие на ЭВМ, образы носителей информации которой создаются (поле Notes) (рис. 6.8).

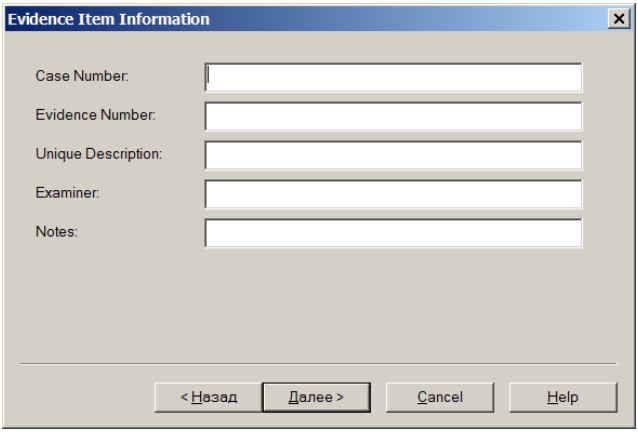


Рис. 6.8. Ввод дополнительной информации

Будет запущен процесс копирования данных, состояние которого отображается в статусном окне. После завершения копирования в поле Status будет отображена строка Image created successfully (рис. 6.9).

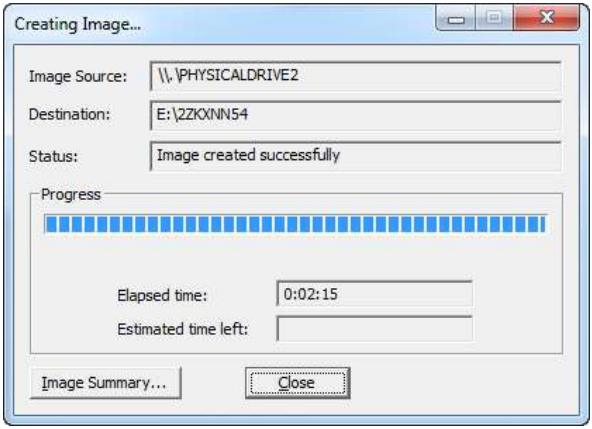


Рис. 6.9. Создание образа

В результате в директории, выбранной для сохранения создаваемого образа, будут записаны два файла: файл-образ и текстовый файл, содержащий дополнительную информацию (рис. 6.10).

Рис. 6.10. Выходные файлы

В последующем полученный образ накопителя может быть исследован с применением специализированных программных комплексов (AccessData Forensic ToolKit, EnCase, AutoPsy и др.), а также развернут на другой накопитель и использован для анализа другими средствами.

После изложенного выше процесса снятия дампов оперативной памяти компьютера и его накопителей можно переходить к фиксации других нижеприведенных текущих данных.

Проверка наличия активных сетевых подключений

Запуск командной строки. В среде MS Windows комбинация клавиш Win + R, затем команда cmd, затем Enter (рис. 6.11).

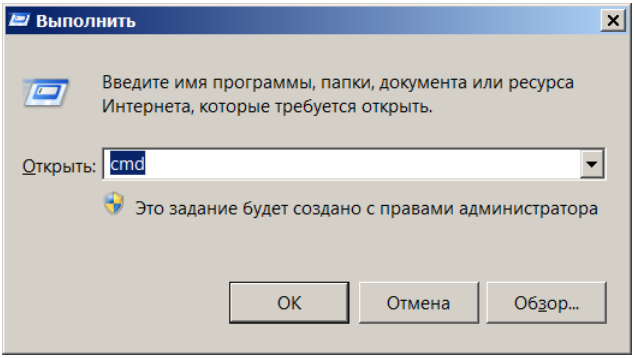


Рис. 6.11. Окно «Выполнить»

В появившемся окне обработчика команд Windows необходимо ввести команду:

netstat –b > F:\connections.txt.

Ключ –b, переданный утилите netstat, позволяет вывести названия исполняемых файлов, которые инициировали данное соединение.

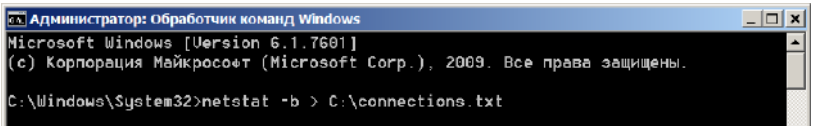


Рис. 6.12. Список активных соединений

В итоге вывод будет записан в файл, который был указан (рис. 6.12).

Вывод состоит из таблицы: в первом столбце – название протокола, во втором – локальный адрес, в третьем – внешний адрес (с кем установлено соединение).

ВНИМАНИЕ! Путь для сохранения данных не должен указывать на локальные диски осматриваемого компьютера. Данные необходимо сохранять на внешнем, заранее подключенном USB-накопителе, например **netstat –b > F:\connections.txt**, где буква диска соответствует подключенному внешнему накопителю. В нижеуказанных примерах принцип указания места записи данных тот же.

Список запущенных процессов и сервисов

Оставаясь в том же окне командной строки, выполнить команду (рис. 6.13):

tasklist /SVC > tasklist.txt.

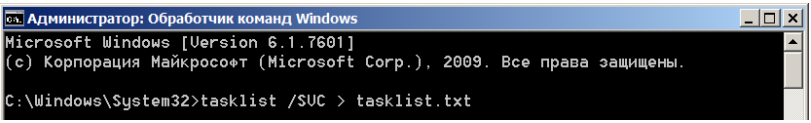


Рис. 6.13. Список процессов и сервисов

В итоге вывод будет записан в файл, который был указан.

Копирования кэша DNS

Оставаясь в том же окне командной строки, выполнить команду (рис. 6.14).

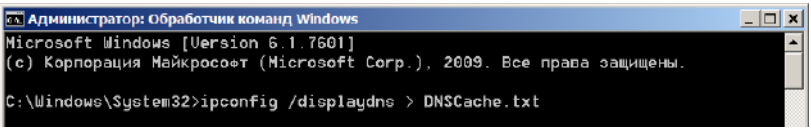


Рис. 6.14. Вывод кэша DNS

В итоге вывод будет записан в файл, который был указан.

Просмотр сетевых подключений

В ОС MS Windows список активных сетевых интерфейсов можно просмотреть в Пуск – Панель управления – Сеть и интернет – Центр управления сетями и общим доступом – Изменение параметров адаптера (рис. 6.15).

На данной странице будут перечислены все сетевые интерфейсы.

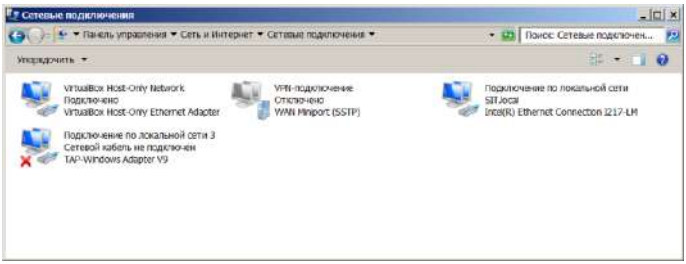


Рис. 6.15. Сетевые подключения

Отключенные сетевые интерфейсы будут отмечены красным крестом. Неактивные сетевые интерфейсы обозначены серым цветом и имеют статус «Отключено». Активные сетевые подключения имеют статус «Подключено» либо название сети, к которой они подключены.

Просмотр состояния активных сетевых подключений выполняется вызовом контекстного меню на требуемом сетевом подключении и выбором пункта «Состояние» (рис. 6.16).

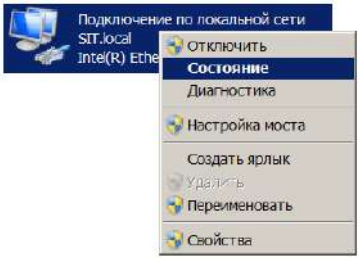


Рис. 6.16. Сетевое подключение

В окне «Состояние» будут указаны длительность подключения и объем переданных (полученных) данных. Далее необходимо нажать кнопку «Сведения» (рис. 6.17). В появившемся окне будет приведена информация о текущем сетевом интерфейсе.

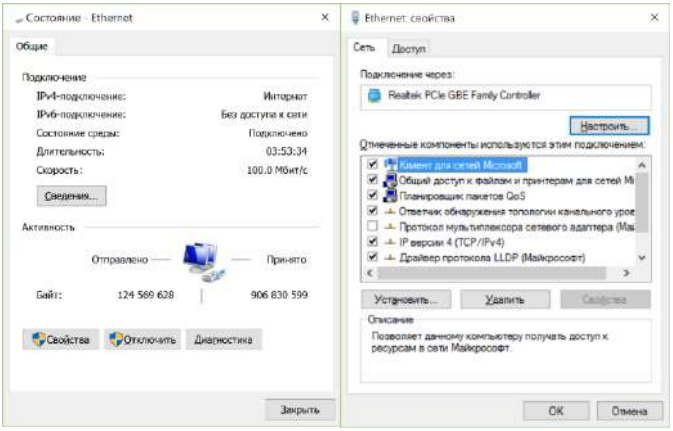


Рис. 6.17. Свойства сетевого адаптера

В окне «Сведения» (рис. 6.18) будет указана информация: о текущем IP-адресе компьютера; о типе распределения адресов в данном сегменте исследуемой локальной сети; об IP-адресах DHCP-, DNS-серверов.

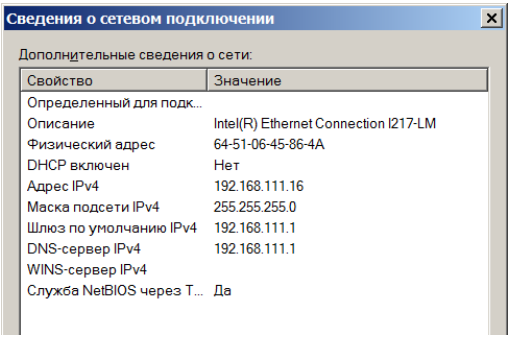


Рис. 6.18. Свойства сетевого подключения

Определение конфигурации протокола TCP/IP

В окне конфигурации сети выберите «IP версии 4 (TCP/IPv4)» и нажмите кнопку «Свойства». Откроется окно настройки параметров протокола TCP/IP. В данном окне откройте закладку «IP-адрес». В данном окне может отсутствовать какая-либо информация о текущих настройках протокола. Это свидетельствует о том, что установлен режим автоматического получения сетевых настроек с DHCP-сервера (рис. 6.19).

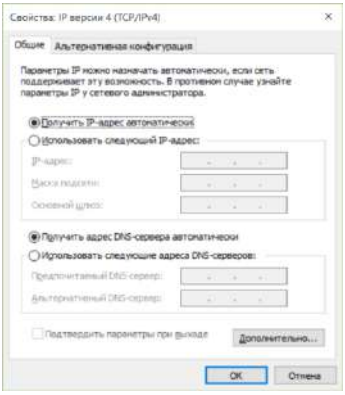


Рис. 6.19. Свойства IPv4

Для просмотра текущей конфигурации протокола TCP/IP воспользуйтесь программой ipconfig, входящей в состав ОС Windows. Программа является консольной, поэтому для ее выполнения необходимо в командной строке консоли вызвать программу **ipconfig**, передав ей ключ /all (рис. 6.20).

Рис. 6.20. Ipconfig

Анализ маски подсети позволяет оценить размеры данного сегмента сети – так как маска 255.255.255.0, значит, в IP-адресе первые три числа (192.168.105) определяют адрес подсети, а последнее

число (например, 10) – адрес компьютера в данной подсети. Следовательно, в данном сегменте сети может быть не более 254 компьютеров с адресами 192.168.105.1 – 192.168.105.254.

С уверенностью можно сказать о существовании двух компьютеров – данного компьютера (имеет адрес 192.168.105.10) и основного шлюза с адресом 192.168.105.200.

Логически сеть состоит как минимум из двух сегментов: один из них – это сеть с адресами 192.168.105.xxx, в которой расположен данный компьютер, второй сегмент – сеть с адресами 192.168.1.xxx, в которой расположен компьютер с адресом 192.168.1.1, совмещающий в себе функции DNS-, DHCP- и WINS-сервера.

На экране отобразится окно, в котором выведены все настройки протокола IP.

Данная информация позволяет сделать ряд выводов: в данной локальной сети используется динамическая система распределения адресов, адрес получен с сервера DHCP, имеющего адрес 192.168.1.1.

ВНИМАНИЕ! Все указанные выше сведения из окон графического интерфейса (если они предположительно имеют криминалистическую значимость) переносятся, как правило, вручную в протокол следственного действия. Фиксация путем создания снимков с экрана возможна, однако только средствами мобильного графического редактора, запущенного с подключенного внешнего накопителя. Категорически запрещается использовать для сохранения снимков с экрана программные средства осматриваемого компьютера (Paint, Adobe Photoshop, Microsoft Word и др.), поскольку это будет отражено в реестре и журналах ОС. Также нельзя делать скриншоты до снятия образа оперативной памяти, так как их содержимое будет включено в файл дампа.

Отключение сетевых соединений

Производится путем извлечения сетевых кабелей с интерфейсом RJ-45 из порта сетевого адаптера (рис. 6.21).

В случае обнаружения беспроводных сетевых интерфейсов (они могут быть выполнены в форме USB-флеш-накопителя и находиться в USB-портах компьютера спереди или сзади) необходимо их извлечь. В случае обнаружения антенн в задней части системного блока (Wi-Fi-адаптер) необходимо открутить эти антенны либо отключить сетевой интерфейс в панели управления (рис. 6.22).

Рис. 6.21. Порты материнской платы и сетевой кабель

Рис. 6.22. PCI Wi-Fi-адаптер

Выключение компьютера

В случаях изъятия работающего компьютера возникает вопрос о способе завершения его работы и отключения от сети питания. Существует два способа, имеющих право на существование в зависимости от конкретных обстоятельств дела.

Первый способ – процедура завершения работы компьютера, предусмотренная его ОС.

Второй – отключение питания (кнопкой на корпусе, извлечением шнура питания из розетки, извлечением аккумулятора из ноутбука).

Вопреки распространенному мнению, при аварийном отключении питания по второму варианту никаких критичных сбоев в ОС и логической структуре накопителей персонального компьютера не произойдет, но будут сохранены временные данные, которые, как правило, удаляются при традиционном способе выключения компьютера.

Исключением являются серверные системы, выключение которых путем аварийного прекращения питания может повлечь повреждение целостности дисковой подсистемы из-за некорректного размонтирования разделов. Поэтому такие системы (серверы интернет- и хостинг-провайдеров, кредитных организаций, промышленных предприятий и т. п.) должны выключаться предусмотренным ОС способом, при необходимости – с участием IT-специалиста данной организации.

В любом случае необходимо четко представлять, какие последствия может иметь тот или иной способ отключения компьютера. Вариантов может быть достаточно много: от наличия системы шифрования на накопителе, которая закроет доступ к данным после выключения компьютера и извлечения НЖМД, до применения пользователем скриптов или заданий планировщика, выполняемых параллельно с выключением компьютера (удаление временных файлов, конкретных каталогов, форматирование накопителя и т. д.). Поэтому решение о способе выключения и изъятия компьютера должен принимать специалист по согласованию с лицом, ответственным за проведение следственного действия или оперативного мероприятия.

§ 6.2. Восстановление и поиск компьютерной информации

ВНИМАНИЕ! Все нижеописанные действия, проводимые с использованием графического интерфейса и системного программного обеспечения, осуществимы и допустимы только в следующих случаях:

– запуск ОС на стендовом компьютере эксперта или специалиста с накопителя, на который был развернут ранее снятый с исследуемого накопителя образ;

– запуск ОС с ранее снятого образа накопителя посредством виртуальной машины (Microsoft VmWare, Oracle VirtualBox);

– просмотр содержимого копии исследуемого накопителя как съемного диска, подключенного к стендовому компьютеру эксперта (специалиста).

Фиксации подлежит информация обо всех доступных на исследуемом компьютере носителях информации, а именно: буква и метка логического диска, его объем. Для этого, открыв Проводник – Мой компьютер, необходимо перечислить все устройства, диски, а также ресурсы локальной сети, подключенные к компьютеру (рис. 6.23).

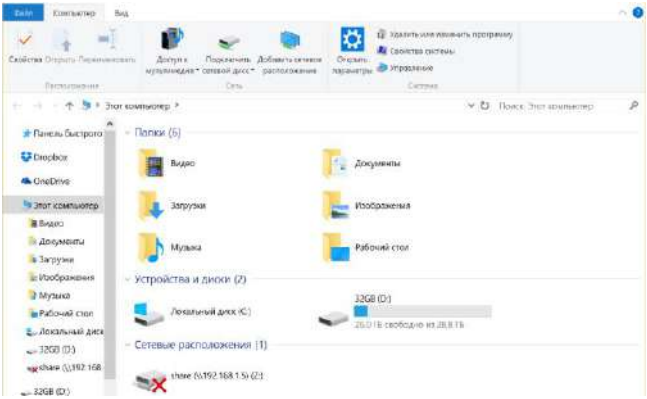


Рис. 6.23. Содержимое «Мой компьютер»

В дальнейшем достаточно вкратце описать содержимое логических дисков (каталоги, файлы), сделать скриншот содержимого логических дисков, отобразив папку в виде таблицы, или сохранить структуру данных диска, используя специальный инструментарий (например, NikFileTree).

Углубленный анализ накопителя на наличие свободных областей, скрытых и шифрованных разделов проводится в лабораторных условиях на стадии производства экспертизы.

Поиск пользовательских данных в ОС Windows

Как правило, в рамках оперативного мероприятия и следственного действия, в том числе и экспертизы, предполагается поиск информации, имеющей значение для расследования дела, представленной в текстовом, графическом, видео- и аудиоформате. Для каждого из этих типов данных существуют особенности их обнаружения и исследования, описание которых в рамках данной работы в силу ее объема привести не представляется возможным и которые известны специалистам в области компьютерной экспертизы.

Отметим, что для экспресс-поиска необходимой информации применяются программные средства, превосходящие по эффективности встроенные средства ОС, поскольку поиск Windows имеет ряд недостатков:

– не всегда учитывается кодировка файла:

а) в файлах *.txt – ищется текст в кодировке ASCII;

б) в файлах *.doc (*.docx) – ищется текст в кодировке Unicode;

– не осуществляется поиск в некоторых типах файлов (*.sys, *.cpp, *.css, *.mp3, *.exe), так как считается, что файлы такого типа текстовой информации априори не содержат.

Спектр альтернативных поисковых средств достаточно широк и может включать в себя все доступные эксперту (специалисту) программные продукты, такие как dtSearch Desktop,

«Ищейка», «Архивариус», Google Desktop Search, Yandex Desktop Search, Copernic Desktop Search, ISYS Desktop, SearchInform, AvSearch.

Последняя указанная программа наиболее предпочтительна, поскольку эффективно осуществляет поиск в любых файлах по любому ключевому слову (фрагменту) и имеет криминалистический уклон в части фиксации и оформления результатов поиска. В целом же выбор программы осуществляется на усмотрение эксперта; единственное требование – это применение не менее двух различных программ для проверки достоверности результатов поиска.

Поиск любого типа данных имеет свою специфику, которую можно проиллюстрировать на примере проблем поиска текстовой информации:

– хранение графического изображения текстового документа в файле Microsoft Word;

– хранение текста в виде графического изображения (отсканированный или сфотографированный документ).

В таких случаях контекстный поиск по ключевому слову результатов не даст, что требует применения других методов и, следовательно, обязательного привлечения специалиста при проведении осмотра содержимого накопителя или назначения экспертизы – даже по такому, казалось бы, банальному поводу, как поиск текстовой информации.

Поиск и анализ артефактов ОС Windows для получения доказательств

Правильный и грамотный анализ компьютерных инцидентов необходим для решения поставленных перед экспертом задач. Специалист должен уметь анализировать артефакты ОС Windows на предмет наличия в них следов компьютерных преступлений, чтобы уметь воссоздать ясную картину произошедшего: какой пользователь совершал действия, какие это действия, когда он их совершал, каков механизм и т. п.

Ниже приведен примерный, далеко не исчерпывающий перечень артефактов ОС Windows, изучение которых позволит установить события, происходившие в системе. Они являются своеобразными маркерами, которые помогут ответить на важные вопросы расследования компьютерных инцидентов:

– служебные каталоги Windows (Users, AppData, ApplicationData, Cookies, Local Settings, Temp и т. д.);
– $Recycle.Bin («Корзина»);
– малый дамп памяти (Windows\Minidump);
– файл hosts (WINDOWS\system32\drivers\etc);
– файл гибернации (hiberfil.sys);
– системные журналы *.evt – приложений, системы и безопасности (WINDOWS\system32\config);
– реестр Windows (WINDOWS\system32\config);
– лог-файлы *.log ОС;
– файлы cookie;
– inf-файлы;
– lnk-файлы;
– файлы графических миниатюр Thumbs.db (файл в каталоге, где хранятся файлы изображений; сохраняется даже в случае удаления исходного графического файла);
– файлы очереди печати *.shd и *.spl;
– кэш интернет-браузеров;
– загрузчики файлов (открытие (сохранение) MRU);
– вложения электронной почты – в случае, если работа с ней происходила посредством почтового клиента (файлы данных MS Outlook, найденные в этих местах, включают *.ost и *.pst);
– история Skype (%USERPROFILE%\AppData\Roaming\Skype\<skype-name>);
– загрузки (папка «Загрузки» и соответствующие лог-файлы браузеров);

– альтернативные потоки данных (в частности, Zone.Identifer для файлов: 0 – локальный компьютер, 1 – интранет, 2 – доверенный источник, 3 – интернет, 4 – недоверенный источник);

– Windows Prefetch (функция повышения производительности системы путем предварительной загрузки кодовых страниц часто используемых приложений; одновременно фиксирует в файле с расширением .pf обращение к исполняемым файлам);

– последние открытые файлы Office.

Восстановление удаленных данных

Следует понимать, что восстановление данных – это не возвращение системы в одно из первоначальных состояний, а именно восстановление файлов, удаленных в результате форматирования накопителя, логических ошибок, действий пользователя или вредоносных программ.

При этом широко распространенное в среде рядовых пользователей удаление файла в «Корзину», по сути, таковым не является, так как представляет собой временное перемещение файла в папку Recycle.Bin с последующим восстановлением или окончательным удалением. При таком «удалении» объем занятого (свободного) пространства накопителя не изменяется.

При удалении файла в его классическом смысле происходит внесение в файловую запись файловой системы сведений о том, что пространство, занятое файлом, больше не используется и условно свободно, при этом файл перестает отображаться в структуре данных («Проводнике»), и свободное пространство диска увеличивается на величину удаленного файла. Однако сами данные файла (текстовое, графическое и другое содержимое) физически не стираются и продолжают храниться на накопителе до тех пор, пока не будут перезаписаны другими данными по исчерпании свободного места на диске.

Именно по этой причине существует возможность восстановления удаленных данных как вручную (при наличии соответствующей квалификации), так и специальными программными

средствами, такими как Easy Recovery, GetDataBack, R-Studio (рис. 6.24) и др.

Однако следует понимать, что возможность качественного восстановления данных напрямую зависит от причины и способа их удаления.

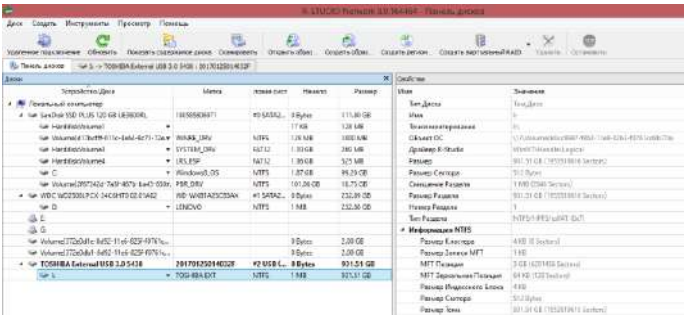


Рис. 6.24. Рабочее окно программы R-Studio с перечнем имеющихся в системе физических и логических дисков

Немаловажным является тот факт, что при восстановлении удаленных данных они не появляются на прежнем месте, а копируются на другой носитель. В ходе анализа содержимого накопителя указанные программы позволяют просмотреть доступное содержимое накопителя, однако не всегда очевидно, какие данные из отображаемых являются удаленными, поэтому зачастую эксперту приходится проводить копирование на другой накопитель всех данных и только после этого сравнивать их с исходным содержимым. В таком случае следует подбирать в качестве целевого диск большего объема, чем объем занятого пространства на исследуемом диске, поскольку восстановленных данных может оказаться значительно больше, чем явно отображается на накопителе. Происходит это по причине того, что зачастую из-за ошибок в файловой системе некоторые файлы восстанавливаются в гораздо большем объеме (например, файл формата .doc объемом 800 Мб), потерянные кластеры и фрагменты перезаписанных файлов преобразуются в самостоятельные файлы.

По аналогии с задачей поиска информации при восстановлении данных следует использовать как минимум два разных программных продукта в целях проверки достоверности полученного результата. Также в рамках одной программы следует применить разные способы восстановления: после форматирования, после удаления пользователем, после сбоя в системе, восстановление по сигнатурам данных.

Восстановление удаленных файлов в файловых системах, отличных от используемых в Windows (Linux, FreeBSD, BeOS, MacOS), производится аналогично. Однако программа восстановления должна поддерживать различные файловые системы, при этом некоторые программы требуют прямого выбора в настройках типа файловой системы.

При неправильном выборе файловой системы программа либо изначально не обнаружит логических разделов на диске, либо (что более критично) проведет сканирование по указанным экспертом параметрам, однако данных не обнаружит, что может повлечь за собой ложный вывод об отсутствии на исследуемом диске удаленных данных.

В случае критических ошибок в файловой системе или физических повреждений поверхности магнитных дисков накопителя, блоков магнитных головок для восстановления данных следует применять программно-аппаратный комплекс отечественного производства PC-3000.

Физические повреждения флеш-накопителей также требуют особых подходов к восстановлению их работоспособности (восстановление разъемов, дорожек платы, извлечение микросхемы памяти и др.).

§ 6.3. Поиск цифровых следов в системах дистанционного банковского обслуживания (ДБО)

События, происходящие в сфере ДБО, традиционно являются объектом пристального внимания служб безопасности банков, применяющих различные типы антифрод-систем для противодействия преступным посягательствам в режиме реального времени.

Большинство систем ДБО были разработаны финансовыми организациями самостоятельно, при этом в среднем на каждую систему ДБО приходилось до 5–7 некритичных уязвимостей. В последнее время наблюдается тенденция к повышению надежности систем сторонних производителей по сравнению с банковскими продуктами. Тем не менее наиболее распространенными уязвимостями онлайн-банков традиционно являются:

– межсайтовое выполнение сценариев;

– недостаточная защита от атак, направленных на перехват данных, которые позволяют совершать атаки на клиентов банков (например, перехватывать значения cookie или похищать учетные данные);

– недостаточная авторизация, позволяющая злоумышленнику получить несанкционированный доступ к функциям веб-приложения, не предназначенным для данного уровня пользователя.

Реакция служб безопасности финансовых организаций на инциденты, связанные с применением именно компьютерных технологий и происходящие в режиме реального времени, направлена на оперативное установление местонахождения злоумышленника и предотвращения преступных действий. Происходит это, как правило, при несанкционированном доступе непосредственно к системе банка. При достаточной квалификации сотрудников службы IT банка возможно установление практических сведений, достаточных для идентификации терминала, с которого осуществляется доступ, а в некоторых случаях и злоумышленника.

Однако чаще всего инцидент исследуется уже постфактум, после наступления последствий и возбуждения уголовного дела по заявлению клиента о списании денежных средств со счета. Нередко данные о доступе извне либо уничтожены самим злоумышленником, либо перезаписаны в ходе наполнения лог-файла сервера. В таком случае исследованию подлежат носители информации, содержащие следы преступного посягательства, находящиеся на компьютерах (удаленных терминалах) и мобильных устройствах пользователей.

В качестве примеров можно привести:

– внедрение в компьютеры и гаджеты пользователей вредоносных программ и троянов, позволяющих злоумышленникам использовать установленные приложения онлайн-банкинга;

– внедрение вредоносных программ, подменяющих банковские реквизиты в платежных поручениях юридических лиц в момент их сохранения и передачи по сети в банк;

– использование пользователем фишинговых сайтов, оформленных под официальные страницы банков и передающих учетные данные пользователей злоумышленникам.

Так или иначе, ключевым вопросом в получении информации о событии является установление последовательности действий пользователя и программ на компьютере с ДБО. Провести такой анализ в условиях оперативного мероприятия или осмотра с участием специалиста, как правило, не представляется возможным, поскольку требует значительных временных затрат, поэтому осуществляется уже в рамках компьютерной экспертизы.

Наиболее эффективным средством в данном случае является построение цепочки произошедших событий в заданном диапазоне дат с использованием технологии timeline, заключающейся в извлечении временных меток из всех возможных хранилищ (метаданных файлов, лог-файлов, скрытых потоков, записей файловой системы) и их упорядочивании в хронологическом порядке.

Существует достаточно широкий спектр криминалистических программных средств, доступных экспертам для реализации указанного метода. В среде Linux это, например, LogTo-Timeline и AutoPsy, в среде Windows – 4n6time и программный комплекс Belkasoft Evidence Center (рис. 6.25).

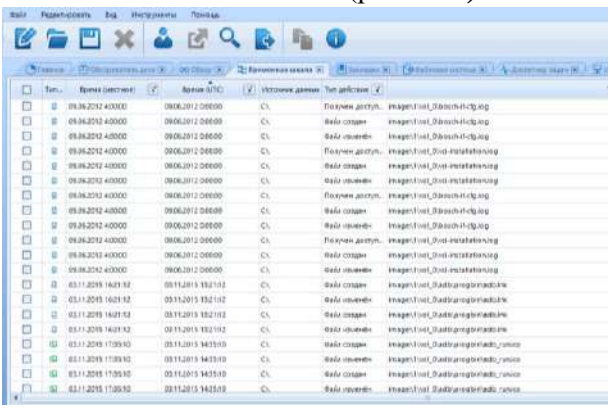


Рис. 6.25. Фрагмент рабочего окна программного комплекса Belkasoft Evidence Center с открытой вкладкой «Временная шкала» (timeline)

После получения последовательности событий эксперт путем ручного анализа или применения фильтров выявляет аномалии (создание, изменение, удаление файлов), свидетельствующие о вредоносном воздействии на компьютерную систему. Привести конкретный перечень следов не представляется возможным, так как в каждом конкретном случае следовая картина может отличаться от аналогичных. К типичным следам, которые могут свидетельствовать о внедрении вредоносных программ в систему, можно отнести:

– открытие пользователем исполняемого или OLE-файла из сообщения электронной почты с последующим запуском процесса в оперативной памяти, изменением значений ключей реестра и др.;

– запуск исполняемого файла или файла сценария в результате обработки автозапуска съемного накопителя;

– запуск VBS-скрипта из каталога пользователя;

– запуск исполняемого файла системы «банк – клиент» в период времени, не характерный для обычной пользовательской активности;

– запуск исполняемых файлов и библиотек, обращавшихся к модулям системы «банк – клиент».

Сложность обнаружения подобных следов заключается в том, что для их вычленения из ряда событий, представленных во временной шкале, требуется наличие у эксперта (специалиста) базовых знаний о принципах функционирования наиболее распространенных систем ДБО, вредоносных программ, эксплойтов, троянов, бухгалтерских программ (1С, «Парус»).

§ 6.4. Особенности назначения компьютерных экспертиз

Судебная компьютерная экспертиза[1] относится к классу инженерно-технических экспертиз и призвана решить задачу поиска компьютерной информации по заданным параметрам. Исследуются различные носители, информация на которых представлена в виде файловых систем, например информация,

[1] Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (вместе с Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации) (ред. от 27.06.2019) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_55315.

содержащаяся в мобильном оборудовании сетей сотовой связи стандарта GSM[1].

На практике возникает путаница с наименованием вида экспертизы, поскольку традиционно выделяют четыре рода таких экспертиз:

1. Аппаратно-компьютерная экспертиза.
2. Программно-компьютерная экспертиза.
3. Информационно-компьютерная экспертиза (данных).
4. Компьютерно-сетевая экспертиза[2].

Судебная компьютерная экспертиза по исследованию компьютерной информации (более общее название, чем приведенное выше) производится в экспертно-криминалистических подразделениях МВД России. В экспертных учреждениях других министерств[3] и ведомств, а также при производстве негосударственной экспертизы она носит название «компьютерно-техническая». Так, исследование компьютерного оборудования (аппаратной части) должно быть назначено в другие экспертные учреждения (государственные и негосударственные), а также конкретным экспертам.

Однако этот факт не должен вводить в заблуждение назначающего судебную экспертизу. На практике суды зачастую

---

[1] См., например: Типовая методика исследования информации, содержащейся в мобильных телефонах / [О. В. Тушканова и др.]. М. : ЭКЦ МВД России, 2014. С. 3.

[2] Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М. : Право и закон, 2001. С. 121. Более подробно о видах экспертиз см.: Шаевич А. А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений : монография. Иркутск : Восточно-Сибирский институт МВД России, 2011.

[3] См., например: Компьютерно-техническая экспертиза // РФЦСЭ при Минюсте России. URL: http://www.sudexpert.ru/possib/comp.php.

не усматривают разницы в наименованиях экспертиз: «Наименования экспертизы „компьютерная" и „программно-техническая" суд считает тождественными»[1].

Важно помнить, что следователю необходимо заранее согласовать свои действия по назначению судебной экспертизы с экспертным учреждением или конкретным экспертом, которому эта экспертиза будет назначена. Это существенно сэкономит силы и средства, а также время, затрачиваемое на производство экспертизы.

Кроме того, в зависимости от задач следствия возможно проведение комплексных судебных экспертиз, например с привлечением специалистов в области криптографии и защиты информации или видеотехники при исследовании видеозаписей, произведенных или обработанных с помощью компьютерных средств и программного обеспечения.

Следует заметить, что в последнем случае следователи зачастую допускают ошибку: на экспертизу представляется аутентичный файл (копия исходного файла), где видеозапись зафиксирована одним целым файлом. В этом случае выявить признаки монтажа записи не представляется возможным. Наличие же программного обеспечения, предназначенного для монтажа видеозаписи, не является доказательством того, что монтаж имел место.

Традиционно назначение любой судебной экспертизы в уголовном судопроизводстве складывается из ряда этапов:

1. **Принятие решения о необходимости назначения судебной экспертизы.** Согласно УПК РФ назначение судебной экспертизы производится в случае необходимости (ч. 1 ст. 195). То есть из постановления о назначении судебной экспертизы должно быть видно, что у следователя такая необходимость воз-

[1] Приговор № 1-115/2019 от 20 сентября 2019 г. по уголовному делу № 1-87/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. URL: http://sudact.ru/regular/doc/eCrzfkGLkMl6.

никла, например, в связи с установлением определенных обстоятельств преступления, изъятием объектов и возникшей необходимостью их исследования в целях поиска компьютерной информации.

Так, согласно приговору «…потерпевшая показала, что она имеет две банковские карты, к которым подключена услуга „Мобильный банк" на абонентский номер №… Она сдала свой мобильный телефон на ремонт. Сим-карту с абонентским номером… из данного телефона она изъяла и поставила в другой принадлежащий ей смартфон… По банковской выписке она увидела, что на счет ее карты поступила заработная плата в сумме… рублей, при этом… денежные средства были сняты в сумме… рублей, однако она данные денежные средства не снимала. Карта на момент снятия денег находилась при ней. Картой пользовалась только она. Пин-код никто, кроме нее, не знал. В момент снятия с ее банковской карты денежных средств ей никаких SMS-сообщений не поступало, код подтверждения данных операций также не приходил <…>.

В ходе выемки у потерпевшей изъят смартфон, который осмотрен, признан и приобщен к уголовному делу в качестве вещественного доказательства»[1].

В другом деле «…в ходе осмотра места происшествия было обнаружено, что в процессах компьютера В. В. Семенова запущен процесс под названием „TeamViewer", который используется для осуществления удаленного доступа к компьютеру, НЖМД, установленный в компьютере В. В. Семенова, был изъят и направлен для проведения компьютерной экспертизы»[2].

---

[1] Приговор по уголовному делу № 1-18/2018 (1-528/2017) // ГАС «Правосудие». URL: https://bsr.sudrf.ru.

[2] Решение № 2-3192/2019 2-3192/2019~М-2853/2019 М-2853/2019 от 27 августа 2019 г. по гражданскому делу № 2-3192/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. URL: http://sudact.ru/regular/doc/boeC5NN2AR1S.

Мотивом назначения компьютерной экспертизы выступает необходимость применения специальных знаний в области исследования компьютерной информации.

Мотив должен быть отражен в постановлении о назначении судебной экспертизы.

2. **Выбор экспертного учреждения или конкретного эксперта.** Судебная компьютерная экспертиза, как правило, назначается в экспертно-криминалистические подразделения МВД России.

При предварительной беседе с экспертом необходимо обозначить ему обстоятельства и вид обнаруженных объектов, задачу по обнаружению компьютерной информации, уточнить возможности эксперта. Экспертом могут быть определены дополнительные условия, при которых объект возможно подвергнуть исследованию с минимальными затратами времени, например получить код разблокировки мобильного телефона и т. д.

Экспертиза может быть назначена и в иные государственные[1] и негосударственные экспертные учреждения, некоммерческие организации, экспертные ассоциации, а также конкретным негосударственным экспертам.

Необходимо иметь в виду, что п. 5 постановления Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам» (далее – ППВС № 28 «О судебной экспертизе») предусматривает конкретные обстоятельства, при которых экспертиза невозможна в государственном судебно-экспертном учреждении, обслуживающем определенную территорию «…в связи с отсутствием эксперта конкретной специальности или надлежащей материально-технической базы либо специальных условий для выполнения исследований, а также при наличии обстоятельств, указанных в ст. 70 УПК РФ, т. е. когда все компетентные государственные

[1] См., например: Компьютерно-техническая экспертиза. URL: http://www.sudexpert.ru/ possib/comp.php.

судебно-экспертные учреждения на данной территории не могут выступить в этом качестве…».

При выборе конкретного эксперта необходимо установить его компетентность. Это обстоятельство устанавливается исходя из наличия у эксперта соответствующего образования, стажа работы в экспертной должности, стажа производства судебно-компьютерных экспертиз и «…иных данных, свидетельствующих о его компетентности и надлежащей квалификации» (абзац второй п. 3 ППВС № 28 «О судебной экспертизе»).

Федеральным законом от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» установлены квалификационные требования к государственным экспертам, которым они должны соответствовать. В судах зачастую выясняют уровень образования, какую **конкретно** экспертную специальность имеет эксперт, его должность, уровень квалификации, наличие аттестации на право самостоятельного производства судебной экспертизы, дату последней аттестации (один раз в пять лет).

У эксперта, выполнившего компьютерную экспертизу по исследованию компьютерной информации, должно быть соответствующее высшее образование либо, согласно ст. 13 Федерального закона № 73-ФЗ, высшее профессиональное образование и подготовка по соответствующей экспертной специализации. Подтверждением наличия такой подготовки у государственного судебного эксперта является свидетельство на право самостоятельного производства экспертизы, у негосударственного – сертификаты и дипломы о повышении квалификации, профессиональной переподготовке, добровольной сертификации, членстве в саморегулируемой организации и др.

Важно помнить, что при назначении экспертизы негосударственному эксперту велика вероятность подбора некомпетент-

ного специалиста, поскольку, как правило, следователь осуществляет свой выбор через интернет, изучая сайт той или иной экспертной организации или эксперта.

Профессор Е. Р. Россинская в своих публикациях неоднократно подчеркивала, что качество выполняемых исследований и консультаций такими организациями практически всегда не связано с качеством интернет-сайта. Сайт – это не более чем красивая витрина, так называемые эксперты не имеют экспертного образования по специализации «Судебная компьютерно-техническая экспертиза» либо не прошли профессиональную переподготовку: «Зачастую это лица, весьма далекие от судопроизводства, которые руководствуются не экспертными технологиями, а исключительно сведениями из „большой науки", не видят различий между судебно-экспертной и научной деятельностью, не знают азов материального и процессуального права, не всегда осознают юридические последствия данных ими заключений. Во многих случаях подобные эксперты допускают выход за пределы своей компетенции – берутся за решение вопросов, являющихся прерогативой правоприменителя, или вопросов, для ответов на которые вообще не требуется специальных знаний»[1].

Поэтому при анализе компетентности эксперта необходимо выяснить не столько происхождение изучаемого интернет-сайта, сколько качество заключений экспертов, выполненных ранее по аналогичным объектам.

3. **Согласование с экспертным учреждением, экспертом редакции вопросов, которые будут поставлены на экспертизу, составление перечня вопросов.** Своеобразие задач и объектов судебной компьютерной экспертизы ведет к тому, что в каждом конкретном случае следователь вынужден согласовы-

[1] Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 5. С. 39.

вать с экспертом перечень и редакцию вопросов. Во многих работах исследователи приводят перечни вопросов, подлежащих исследованию, в результате чего следователи механически их копируют и размещают в постановлении о назначении судебной экспертизы. Такая практика неприемлема: вопросы не должны быть шаблонными. Однако в качестве ориентира считаем необходимым привести перечни вопросов, которые могут быть поставлены перед экспертами (Приложение 1).

4. **Подбор объектов экспертизы.** Обозначим объекты исследования, при исследовании которых эксперты осуществляют поиск компьютерной информации по заданным критериям[1].

Компьютерная информация, содержащаяся на следующих машинных носителях:

– накопителях на жестких магнитных дисках (НЖМД);

– гибких магнитных дисках (ГМД), zip- и jaz-дисках;

– магнитных лентах;

– CD- и DVD-дисках;

– флеш-накопителях;

– картах памяти и прочих машинных носителях, информация на которых представлена в виде файловых систем.

При исследовании информации в мобильных телефонах[2]:

– информация, содержащаяся в мобильном оборудовании сетей сотовой связи стандарта GSM;

– мобильное оборудование сетей сотовой связи стандарта GSM.

---

[1] Типовые экспертные методики исследования вещественных доказательств : Ч. I / под ред. Ю. М. Дильдина ; общ. ред. В. В. Мартынова. М. : ЭКЦ МВД России, 2010.

[2] Типовая методика исследования информации в мобильных телефонах / [О. В. Тушканова и др.]. М. : ЭКЦ МВД России, 2013.

ЭКЦ УМВД России по Брянской области указывает на возможность исследования следующих объектов[1]:

– любые документы, которые могли быть изготовлены (полностью или частично) с использованием компьютерных систем и средств копирования информации;

– любая компьютерная информация, к которой можно отнести не только информацию на компьютерных носителях, но и информацию, содержащую тексты программ, баз данных и комментарии к ним на любых других носителях (бумага, видео- и аудиозаписи и т. п.);

– компьютерные системы (компьютеры и их компоненты, периферийные устройства, средства связи, компьютерные сети);

– сопроводительная документация к компьютерной и электронной технике;

– технические средства и носители информации, множительная техника, средства связи и спецтехника.

Следователю необходимо представить изъятые в ходе расследования предметы, документы, которые органически отражают взаимосвязь представляемых на экспертизу объектов с преступлением.

ВНИМАНИЕ! На экспертизу может быть представлен только конкретный физический объект, передаваемый эксперту при назначении экспертизы. Иными словами, не могут быть представлены электронный почтовый ящик, облачное хранилище, интернет-сайт, аккаунт в социальной сети и т. д.

И напротив, могут быть представлены физический почтовый сервер, дата-центр, веб-сервер, персональный компьютер, ноутбук, накопитель на магнитных дисках, флеш-накопитель и т. д.

---

[1] Рекомендации по изъятию компьютерной техники и носителей информации при проведении обыска. Варианты описания объектов, содержащих компьютерную информацию : методические рекомендации. Брянск : ЭКЦ УМВД России по Брянской области, 2013. С. 12.

Объекты должны поступить на экспертизу в упаковке, не допускающей возможность повреждения объекта или его изъятия без нарушения целостности упаковки. Особое внимание следует уделить вопросам происхождения объектов, законности их получения, в том числе в результате проведения оперативно-разыскных мероприятий.

5. **Вынесение постановления о назначении судебной экспертизы.** При вынесении постановления необходимо обратить внимание на указание следующих обстоятельств (кроме формальных реквизитов):

– наименование экспертизы. По общим рекомендациям, необходимо приводить родовое название экспертизы – «компьютерная» («компьютерно-техническая»). Это избавит от проблем выяснения при оценке заключения эксперта или в суде законности производства экспертизы, правильности примененных методов, компетенции эксперта и т. п.;

– обстоятельства дела. Например, наличие необходимых данных о месте происшествия – состав сети, состав аппаратных средств и т. д. По согласованию с экспертом следователь определяет объем сведений, который необходимо изложить в постановлении. В зависимости от обстоятельств дела занимают объем 0,5–6 страниц печатного текста. Указываются также обстоятельства проведения оперативно-разыскных мероприятий, их результаты;

– мотив назначения экспертизы – необходимость применения специальных знаний в области компьютерной экспертизы (в области исследования компьютерной информации, в области компьютерных технологий и т. п.). Не следует употреблять фразу «…и принимая во внимание, что для проведения судебной компьютерной экспертизы нужны специальные познания…», поскольку это не мотив назначения экспертизы, а суть самой экспертизы. Интересной представляется ситуация, когда необходимо в целях экспертизы изъять электронные носители информации (п. 1 ч. 1 ст. 164.1 УПК РФ). Логика процесса говорит

о том, что эта деятельность должна осуществляться в обратном порядке – «от объекта к экспертизе». Не вдаваясь в процессуальные споры, отметим, что в этой ситуации при изъятии и направлении на экспертизу электронных носителей информации в качестве мотива следует упомянуть «необходимость назначения судебной компьютерной экспертизы»;

– согласованные с экспертом вопросы: краткие, носящие конкретный характер, исключительно имеющие отношение к делу, с использованием специальной стандартизированной терминологии[1]. Не допускаются вопросы справочного или правового характера, к примеру: «Какие файлы имеются на представленном носителе информации?», «Является ли представленное на экспертизу программное обеспечение контрафактным, какова стоимость лицензионного программного обеспечения?» и т. п.;

– точный перечень представленных на экспертизу объектов, их упаковка, содержание пояснительных надписей (необходимо полное совпадение содержания надписей на упаковке и в соответствующих протоколах следственных действий);

– разрешение на проведение исследований, способных повлечь полное или частичное уничтожение представленных объектов либо изменение их внешнего вида или основных свойств.

Согласно п. 4 ст. 199 УПК РФ, если судебная экспертиза производится вне экспертного учреждения, то следователь вручает постановление и необходимые материалы эксперту и разъясняет ему права и ответственность, предусмотренные ст. 57 УПК РФ.

Чтобы не допустить повреждения или утраты объектов, их транспортировка на экспертизу должна происходить с соблюдением требований безопасности в обращении с ними.

---

[1] ГОСТ Р 57429–2017. Судебная компьютерно-техническая экспертиза. Термины и определения : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2017 г. № 198-ст : введен впервые : дата введения 2017-09-01 // АО «Кодекс». URL: https://docs.cntd.ru/document/1200144960.

§ 6.5. Оценка заключения эксперта

Уголовно-процессуальным законом предусмотрена обязанность дознавателя, следователя, прокурора и суда осуществлять проверку доказательств путем сопоставления их с другими доказательствами, имеющимися в уголовном деле, а также установления их источников, получения иных доказательств, подтверждающих или опровергающих проверяемое доказательство (ст. 87 УПК РФ)[1].

Для решения такой задачи необходимо прежде всего оценить заключение эксперта как доказательство. Согласно ч. 1 ст. 88 УПК РФ заключение эксперта необходимо оценить с точки зрения его относимости, допустимости и достоверности. К сожалению, формально результат такой деятельности никаким процессуальным документом не оформляется.

Отметим два обстоятельства. Судебно-компьютерная экспертиза проводится, как правило, без присутствия следователя, хотя его присутствие возможно (ст. 197 УПК РФ), а заключение эксперта формируется не в результате непосредственной деятельности следователя. Это определяет необходимость подробного описания всех стадий исследования в заключении эксперта для формирования у следователя правильного представления о процессе исследования.

Кроме того, при проведении исследования и даче заключения, а также при составлении заключения экспертом используются специальные знания, выходящие за рамки необходимых профессиональных знаний следователя. Это затрудняет оценку заключения эксперта, поскольку следователь, как правило, не

---

[1] Более подробно см., например: Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. М. : Норма, 2006. С. 268–279 ; Пропастин С. В. Оценка следователем результатов компьютерной экспертизы // Уголовный процесс. URL: https://www.ugpr.ru/article/199-otsenka-sledovatelem-rezultatov-kompyuternoy-ekspertizy.

владеет глубокими знаниями в области исследования компьютерной информации, а анализ текста заключения вызывает затруднения из-за обилия специальной терминологии, сложности описанных процессов и полученных результатов.

Такое непонимание текста заключения ведет к проявлению лени и невнимательности со стороны следователя, игнорированию требований УПК РФ, сведению оценки заключения эксперта к ознакомлению с выводами и сопоставлению количества поставленных вопросов и данных ответов. Ничего из этого недопустимо в принципе.

Важно уяснить, что в подавляющем большинстве случаев ошибки в исследовании выявляются только при тщательном изучении всего заключения эксперта, от его начала и до конца.

Выводы в заключении эксперта как интерпретация и концентрированное выражение промежуточных выводов исследования являются лишь формализованными ответами на вопросы, поставленные перед экспертом. Такое простое сравнение следователем вопросов и ответов ведет к самоуспокоению, неправильному пониманию значения заключения эксперта, подмене сложного процесса оценки полученного потенциального доказательства вредным, халатным, упрощенческим подходом, неким ознакомлением. Представляется, что следователь как профессионал не должен допускать такого проявления безразличия к происхождению доказательства.

В любом случае следователь обязан осуществить глубокую оценку заключения судебно-компьютерной экспертизы во избежание следственных и судебных ошибок.

Следователю необходимо достоверно установить ряд обстоятельств, часть из которых носит общий характер и не зависит от вида проведенной судебной экспертизы:

1. **Соблюдены ли требования закона при назначении экспертизы.** Необходимо решить следующие вопросы:

1.1. *Соблюдены ли права участников уголовного судопроизводства при назначении судебной экспертизы?* Для решения этого вопроса необходимо уяснить, соблюдены ли требования ст. 195 УПК РФ, в частности, ознакомлены ли с постановлением о назначении судебной экспертизы **до ее производства** (п. 9 ППВС № 28 «О судебной экспертизе») подозреваемый, обвиняемый, его защитник, потерпевший, его представитель, разъяснены ли им права, предусмотренные ст. 198 УПК РФ, составлен ли об этом протокол.

Суды прямо указывают на исследование этого обстоятельства при постановке приговора. Кроме того, выясняется, соблюдены ли требования ст.ст. 199–201, 207 УПК РФ.

1.2. *Нет ли нарушений при получении образцов для сравнительного исследования?* Как правило, на компьютерную экспертизу в качестве образцов поступают объекты, полученные в результате проведения оперативно-разыскного мероприятия «проверочная закупка», носящие характер свободных. Такие объекты могут быть получены в результате проведения следственных действий, связанных с изъятием объектов: осмотр места происшествия, обыск, выемка и пр. В связи с этим необходимо проверить законность и обоснованность указанных процедур получения свободных образцов. Особое внимание следует уделить материалам оперативно-разыскной деятельности.

Так, согласно приговору «…вопреки доводам подсудимого результаты оперативно-разыскных мероприятий были получены в соответствии с требованиями закона и свидетельствуют о наличии у подсудимого умысла на совершение инкриминируемых преступлений, сформировавшийся независимо от деятельности сотрудников оперативных подразделений правоохранительных органов… Результаты проведенной оперативно-разыскной деятельности отвечают требованиям, предъявляемым к доказательствам, согласуются с иными исследованными судом доказательствами по делу, в том числе заключениями проведенных по делу

экспертиз, установивших наличие на мобильных телефонах потерпевших программ, в функции которых входят скрытые от пользователя отправка и чтение коротких текстовых сообщений SMS, отправка запросов USSD, сокрытие или удаление коротких текстовых сообщений, обращение к ресурсам в сети «Интернет» для получения и передачи какой-либо информации…»[1].

1.3. *Обоснованно и мотивированно ли назначение судебной экспертизы?*

Из постановления о назначении судебной экспертизы должно быть видно, что у следователя такая необходимость возникла, например в связи с установлением определенных обстоятельств преступления, изъятием объектов и возникшей необходимостью их исследования в целях поиска компьютерной информации. В описательной части постановления должны быть указаны только те сведения, которые имеют отношение к экспертизе, например результаты следственных действий, оперативно-разыскных мероприятий и т. п.

Экспертиза может быть назначена также и до возбуждения уголовного дела, причем названия экспертизы в постановлении и заключении эксперта могут различаться, например при исследовании программных продуктов.

Так, приговором суда установлено: «…согласно ч. 1 ст. 144 УПК РФ при проверке сообщения о преступлении орган дознания вправе назначать судебную экспертизу. Поэтому назначение начальником ОМВД России по г. Сухой Лог судебной компьютерной экспертизы соответствует требованиям закона»[2].

1.4. *Правильно ли выбрано экспертное учреждение или конкретный эксперт, нет ли отводов лицу, которому поручено проведение экспертизы (ст. 70 УПК РФ)?* Согласно приказу

---

[1] Приговор по уголовному делу № 1-5/2019 // ГАС «Правосудие». URL: https://bsr.sudrf.ru.

[2] Приговор № 1-115/2019 от 20 сентября 2019 г. по уголовному делу № 1-87/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. URL: http://sudact.ru/regular/doc/ eCrzfkGLkMl6/

МВД России от 29 июня 2005 г. № 511 судебная компьютерная экспертиза по исследованию компьютерной информации проводится в экспертных подразделениях МВД России. В иных случаях может быть выбрано другое место исследования. Основания указаны в п. 5 ППВС № 28 «О судебной экспертизе».

Вопрос оценки правильности выбора конкретного эксперта напрямую зависит от установления его компетенции, о чем будет сказано ниже. Интересным представляется установление факта нахождения эксперта в иной зависимости от сторон или их представителей.

Так, суд указал, что «…между ответчиком и специалистом, осуществляющим составление заключения… экспертизы… ранее имелись правоотношения, основанные на возмездном договоре»[1].

При решении вопроса об отсутствии оснований для отвода эксперту в целях объективности и беспристрастности анализируются сведения, изложенные в вводной части заключения эксперта, касающиеся его личных данных, сведений о месте работы, службы, должности и пр.

По другому делу «…суд апелляционной инстанции считает необходимым исключить… заключение эксперта из числа доказательств, поскольку экспертиза выполнена экспертом, состоящим в родственных отношениях с заместителем прокурора г. Миасса Челябинской области… который в силу занимаемой должности отнесен законодателем к стороне обвинения (п. 47 ст. 5 УПК РФ) и в рамках рассматриваемого уголовного дела в ходе производства предварительного расследования принимал

[1] Постановление Арбитражного суда Центрального округа кассационной инстанции по проверке законности и обоснованности судебных актов арбитражных судов, вступивших в законную силу от 22 января 2020 г. по делу № А83-17242/2017 // СПС «КонсультантПлюс». Режим доступа: по расписанию.

процессуальные решения… что в силу ст.ст. 61, 70 УПК РФ исключает возможность участия эксперта в производстве по настоящему уголовному делу»[1].

1.5. *Правильно ли поставлены вопросы перед экспертом?* В силу специфики и сложности решаемых задач особое значение имеет правильная редакция вопросов эксперту. По общему правилу, вопросы должны относиться исключительно к компетенции эксперта и назначаемой экспертизе и не выходить за их рамки.

Основными ошибками следует назвать использование неустоявшихся терминов (полубытовых, жаргонных и пр.), а также постановку юридических вопросов.

В первом случае необходимо установить, что в вопросах использованы термины согласно, например, имеющимся требованиям стандартов. Во втором случае при постановке на компьютерную экспертизу юридических вопросов (например, является ли объект контрафактным, какова стоимость лицензионного программного обеспечения и пр.) необходимо выяснить, не дал ли эксперт ответ на этот вопрос в своем заключении. Как правило, эксперты ограничиваются фразой, что вопрос о контрафактности не входит в компетенцию эксперта, однако признаки, изложенные в исследовательской части заключения (наличие в составе дистрибутивов файлов с лицензионными ключами и серийными номерами и т. п.), свидетельствуют о нелегальном использовании программных продуктов, содержащихся на исследуемых носителях.

1.6. *Компетентен ли эксперт, проводивший экспертизу?* Как уже отмечалось выше, эксперт должен обладать компетентностью, которая определяется наличием у него высшего образования, стажа экспертной деятельности, в том числе по конкретному виду экспертиз.

---

[1] Апелляционное постановление № 10-5071/2019 от 26 сентября 2019 г. по делу № 10-5071/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. URL: https://sudact.ru/regular/doc/A3mDStHBNax7.

Рассмотрим пример специальности 10.05.01 «Компьютерная безопасность», специализация № 7 «Информационно-аналитическая и техническая экспертиза компьютерных систем». Специалист выполняет поиск, фиксацию, анализ и документирование следов компьютерных преступлений, правонарушений и инцидентов, в том числе экспертизу вычислительной техники и носителей компьютерной информации, с учетом нормативных правовых актов и иных требований.

Специальность 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», специализация № 4 «Компьютерная экспертиза при расследовании преступлений» предполагает производство выпускником судебных компьютерных экспертиз.

То же касается иных специальностей, предусматривающих подготовку судебного эксперта в области компьютерной информации, в том числе в рамках дополнительного профессионального образования, переподготовки и повышения квалификации по утвержденным образовательным стандартам.

Например, в приговоре отражено, что «…допрошенный в судебном заседании эксперт… пояснил, что он работает экспертом в АНО „Первый краевой экспертный центр”». 25 февраля 2019 г. он участвовал в качестве специалиста при проведении сотрудниками ОМВД России по г. Сухой Лог осмотра места происшествия в помещении… При этом на одном из компьютеров были обнаружены установленные программные продукты… на которые не было лицензионных документов и которые запускались при отсутствии ключа аппаратной защиты HASP. Данный компьютер был упакован, изъят и предоставлен ему для проведения экспертизы. В ходе экспертизы он установил, что программные продукты были установлены путем копирования с другого машинного носителя 31 мая 2016 г., поскольку и файловый атрибут каталога с программным продуктом, и файловые

атрибуты файлов в данном каталоге имели значение „дата создания 31 мая 2016 г.”. Последний доступ к базе данных… по журналу регистрации базы данных осуществлен 16 октября 2018 г.»[1]. Из этого можно заключить, что экспертиза проведена в негосударственном экспертном учреждении.

У государственного судебного эксперта должно быть действующее свидетельство на право самостоятельного производства судебной компьютерной экспертизы (срок действия – пять лет).

2. **Оценка процесса экспертного исследования и его результатов.** Для этого осуществляются:

2.1. *Проверка подлинности и достаточности исследовавшихся объектов*. Устанавливаются происхождение исследовавшихся объектов, их пригодность и достаточность для проведения исследования и дачи заключения.

Законность получения объектов экспертизы устанавливается путем анализа документов, отражающих процесс их собирания, т. е. документов оперативно-разыскной деятельности, процессуальной и иной деятельности следователя. Проверяется соблюдение законности при производстве следственных действий и оперативно-разыскных мероприятий.

Объекты в протоколах следственных действий и иных документах должны быть описаны таким образом, чтобы их можно было выделить из группы подобных объектов. Пристальное внимание должно уделяться описанию повреждений, поскольку объект может быть непригоден для исследования. Тем не менее объект подлежит исследованию.

Особое внимание следует уделить сравнению описаний упаковок объектов при их изъятии и осмотре при поступлении на экспертизу. Проверяются целостность упаковки, наличие и соответствие пояснительных надписей.

---

[1] Приговор № 1-115/2019 от 20 сентября 2019 г. по уголовному делу № 1-87/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. URL: http://sudact.ru/regular/doc/ eCrzfkGLkMl6.

После проведения экспертизы эксперт собирает объекты в свою упаковку с сохранением предыдущей упаковки.

Все объекты, поступившие на экспертизу, должны быть исследованы. Недопустимо при исследовании аналогичных электронных носителей информации выяснять характеристики одного объекта и автоматически их же использовать при описании другого, хотя по заводским характеристикам объекты одинаковы. Каждый носитель должен быть исследован полностью.

Достаточность объектов предполагает такое их количество и качество, которое позволило эксперту сделать вывод в процессе решения экспертной задачи. Здесь может идти речь, например, о доброкачественности образцов для сравнительного исследования. Так, для установления сходства электронных документов достаточно иметь один исследуемый файл и один файл – образец для сравнения, чтобы путем сравнения контрольных сумм этих файлов установить их идентичность или аутентичность.

2.2. *Оценка научной обоснованности экспертной методики и правомерности ее применения* в данном конкретном случае. Эти обстоятельства устанавливаются на основе изучения специальной литературы. Однако использовавшаяся методика по меньшей мере должна быть апробирована и внедрена, о чем должны свидетельствовать соответствующие документы.

В каждом конкретном случае при исследовании объектов и решении конкретных экспертных задач необходимо устанавливать, что эксперт пользовался методикой, предназначенной именно для этого вида экспертиз.

При оценке заключения необходимо убедиться, что эксперт строго соблюдал методику исследования, иначе полученные выводы следует признать недостоверными.

Вместе с тем следует учитывать, что в силу ряда объективных причин (в том числе темпов развития науки и техники) сегодня не существует утвержденных, апробированных, сертифицированных методик решения ряда экспертных вопросов как

в сфере компьютерной экспертизы, так и в других развивающихся направлениях экспертной деятельности. Однако это не означает, что такие вопросы не могут быть перед экспертом поставлены или не могут быть им решены.

В условиях отсутствия методики решения вопроса, например о вредоносности программы для ЭВМ, эксперт, если он обладает соответствующими специальными знаниями в области программирования, реверс-инжиниринга, статического и динамического анализа программного кода, обязан как можно более подробно и логично изложить ход и результаты своего исследования – так, чтобы они были понятны всем участникам процесса, не вызывали сомнений в научной обоснованности примененных методов.

Обязательно следует установить факт соблюдения экспертом требований безопасности при работе с компьютерной информацией во избежание ее изменения или утраты.

2.3. *Проверка и оценка полноты и всесторонности заключения*. Складывается из решения вопросов:

а) все ли представленные на экспертизу объекты исследованы?

б) все ли необходимые диагностические и идентификационные признаки выявлены? Следует обратить внимание на непротиворечивость таких признаков признакам, установленным при производстве следственных действий или в ходе оперативно-разыскных мероприятий;

в) использованы ли в исследовании рекомендованные методы и методики, каковы их результаты?

г) даны ли ответы на все вопросы, поставленные перед экспертом, аргументированы ли они? Обоснован ли отказ в даче ответа на вопрос? Так, «…согласно заключению компьютерной экспертизы… определить наличие в памяти мобильного телефона… информации о контактах „телефонной книги”, информа-

ции о принятых, набранных и пропущенных вызовах, информации о сообщениях программ для обмена электронными сообщениями, информации о SMS-сообщениях не представилось возможным, так как С. не предоставил пароль доступа к телефону»[1];

д) полно ли описан в заключении процесс исследования?

е) имеется ли соответствующий иллюстративный материал?

2.4. *Оценка логической последовательности исследования и его результатов* состоит:

а) в анализе стадий экспертного исследования с точки зрения их логической последовательности (описаны в экспертных методиках);

б) наличии логического обоснования выдвинутых промежуточных выводов исследования;

в) наличии логического обоснования окончательных выводов по экспертизе, исходя из наличия промежуточных выводов; установлении отсутствия противоречий между ними и т. д.

3. **Оценка заключения в целом.** Заключается в решении следующих вопросов:

3.1. *Не вышел ли эксперт за пределы своей компетенции*:

а) даны ли ответы в рамках исследования компьютерной информации, а не иного исследования, например криптографического или в области защиты информации?

б) относится ли решение вопросов в рамках экспертной инициативы к проведенному исследованию? К примеру, эксперт исследовал объекты с помощью антивирусного программного обеспечения, результаты чего посчитал необходимым отразить в заключении, хотя соответствующего вопроса перед ним не ставилось;

---

[1] Приговор № 1-118/2019 от 6 сентября 2019 г. по уголовному делу № 1-118/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. URL: http://sudact.ru/regular/doc/b9VnQX8BBENC.

в) не дал ли эксперт ответов на юридические вопросы? Полагаем, что эксперт не может указывать стоимость лицензионного программного обеспечения или указывать на контрафактность объекта исследования в рамках компьютерной экспертизы, – это явно выходит за рамки его компетенции.

3.2. *Соблюдена ли процессуальная форма заключения эксперта*? *Имеются ли необходимые реквизиты?* Следует иметь в виду, что форма заключения судебной экспертизы законодательно не закреплена.

Приведенный ниже перечень из ст. 25 Федерального закона от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» следует использовать как алгоритм проверки формальной стороны заключения, в котором должны быть отражены:

– время и место производства судебной экспертизы;

– основания производства судебной экспертизы;

– сведения об органе или о лице, назначивших судебную экспертизу;

– сведения о государственном судебно-экспертном учреждении, об эксперте (Ф. И. О., образование, специальность, стаж работы, ученая степень и ученое звание, занимаемая должность), которым поручено производство судебной экспертизы;

– предупреждение эксперта в соответствии с законодательством Российской Федерации об ответственности за дачу заведомо ложного заключения;

– вопросы, поставленные перед экспертом или комиссией экспертов;

– объекты исследований и материалы дела, представленные эксперту для производства судебной экспертизы;

– сведения об участниках процесса, присутствовавших при производстве судебной экспертизы;

– содержание и результаты исследований с указанием примененных методов;

– оценка результатов исследований, обоснование и формулировка выводов по поставленным вопросам.

Также в качестве составной части заключения прилагаются иллюстрирующие материалы, которые могут располагаться внутри основного текста и не выноситься в отдельное приложение.

ВНИМАНИЕ! Электронные носители информации как приложение к заключению экспертизы имеют информацию, которая может быть признана вещественным доказательством. Необходимо соблюдать меры предосторожности в обращении с ней.

Заключение должно быть подписано экспертом на каждой странице. Подпись удостоверяется оттиском печати государственного экспертного учреждения.

Выделены структурные элементы заключения эксперта в соответствии со стадиями экспертного исследования, а также сведения, которые отражаются внутри каждого такого элемента (табл. 6.1).

4. **Оценка относимости заключения экспертизы к уголовному делу.** Устанавливается связь полученных в результате исследования выводов с обстоятельствами, подлежащими установлению по уголовному делу.

5. **Оценка соответствия заключения судебной экспертизы другим материалам уголовного дела.** Выводы эксперта не должны противоречить материалам дела. В противном случае либо выдвинутая по делу версия не нашла своего подтверждения, либо имеет место экспертная ошибка[1]. В таком случае возможен либо отказ от версии, либо назначение повторной судебной экспертизы.

[1] Подробнее об ошибках при производстве судебных экспертиз см.: Судебная экспертиза: типичные ошибки / под ред. Е. Р. Россинской. М. : Проспект, 2019.

Таблица 6.1

Структурные элементы заключения эксперта

Часть заключения	**Фиксируемая в заключении информация**
Вводная	− наименование экспертного учреждения; − номер и место составления заключения; − время производства экспертизы; − краткие сведения об эксперте (экспертах); − сведения об органе и лице, назначившем экспертизу, правовых основаниях ее назначения (постановлении, определении и т. п.); − номер и наименование дела, по которому назначена экспертиза;
Вводная	− краткое описание обстоятельств дела, имеющих отношение к экспертизе (из постановления); − род и вид экспертизы; − подписка эксперта (экспертов) об уголовной ответственности за дачу заведомо ложного заключения; − поступившие на экспертизу объекты и материалы, способ их доставки, наличие упаковки и т. п.; − вопросы, поставленные перед экспертом; − примененные методики исследования с указанием литературы, в которой они описаны; − описание и характеристики примененных технических средств
Исследовательская	− вид упаковки представленных на экспертизу объектов, их состояние; − описание объектов в целом; − описание образцов для сравнительного исследования; − процесс исследования по стадиям с описанием его методов, условий применения тех или иных методов, технических средств и их характеристик; − описание оценки результатов исследования, обоснование и формирование выводов, в том числе причин, по которым невозможно дать ответ на вопрос; − обобщение результатов при проведении комплексной экспертизы; – описание упаковки объектов
Выводы	− краткие, однозначные ответы на вопросы, поставленные перед экспертом;

Часть заключения	Фиксируемая в заключении информация
	− причины, по которым невозможно дать ответ на поставленный вопрос; − ответы на вопросы в рамках экспертной инициативы; − подпись эксперта
Приложения	− фототаблицы, иллюстрации; − изображения, изготовленные с помощью компьютерной техники; – электронные носители информации с результатами экспертизы

ГЛАВА 7. Криминологический анализ преступлений в сфере информационных технологий

§ 7.1. Современное состояние преступлений в сфере информационных технологий

Криминологический анализ преступлений основан на изучении и измерении различных параметров, формирующих знание об объекте исследования.

Современное формирование правоприменительной практики по делам о преступлениях в сфере информационных технологий, проблемы статистического учета лишь отчасти позволяют оценить состояние, структуру и динамику преступлений в сфере информационных технологий. Статистика количественных и качественных характеристик состояния преступности в сфере информационных технологий сегодня не имеет достоверного и объективного отражения в силу особой сферы совершения преступлений и складывающейся разнообразной практики выявления, раскрытия и расследования данных преступных посягательств.

Начиная с 2017 г. в статистической отчетности о состоянии преступности в России появился показатель, характеризующий количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (рис. 7.1).

За три года количество зарегистрированных преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, увеличилось более чем в три раза. За 2019 г. удельный вес зарегистрированных преступлений в сфере информационных технологий увеличился практически в два раза – с 174 674 (8,8 %) в 2018 г. до 294 409 (14,5 %),

из которых было раскрыто 22,2 %. Почти половина зарегистрированных преступлений относится к категориям тяжких и особо тяжких (142 728; 48,5 %).

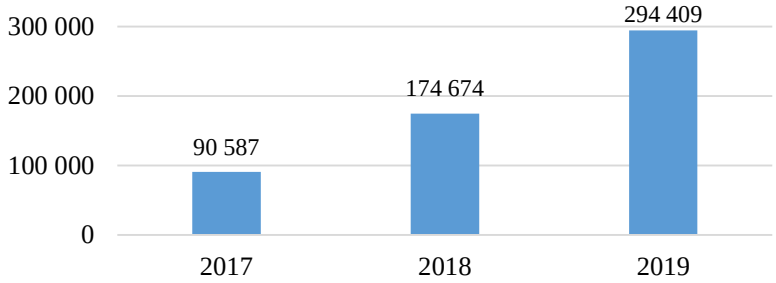


Рис. 7.1. Количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, 2017–2019 гг.

За январь – сентябрь 2020 г. выявлено 363 034 преступления в сфере информационно-телекоммуникационных технологий (за тот же период 2019 г. – 205 116, **прирост – 76,9 %**)[1]. Основным фактором значительного прироста выступает пандемия COVID-19.

Сегодня действуют всеобъемлющие меры социального дистанцирования. Это привело к значительному увеличению использования онлайн-коммуникаций государственными органами, предприятиями и частными лицами. Многие граждане не знакомы с онлайн-технологиями в должном объеме. Все это дало большой, привлекательный и уязвимый набор целей для использования их киберпреступниками. Воздействие пандемии COVID-19 на преступность в сфере информационных технологий наиболее

[1] Ф4 – ЕГС (494). Книга 31. Раздел 11 «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации» // Сборник по России, январь – апрель 2019 г., январь – сентябрь 2020 г.

заметно по сравнению с другими видами преступной деятельности. Характеристики преступлений в сфере информационно-телекоммуникационных технологий выглядят следующим образом:

1. С использованием интернета – 157 036 (48,2 %).
2. С помощью средств мобильной связи – 116 154 (35,6 %).
3. С помощью расчетных (пластиковых) карт – 34 383 (10,6 %).
4. С помощью компьютерной техники – 18 261 (5,6 %).

Фиксируется стабильный рост преступлений в сфере информационных технологий против здоровья населения и общественной нравственности. В 2019 г. зарегистрировано 24 677 таких преступлений (+ 31,2 % по сравнению с 2018 г.), или 8,3 % от общего числа рассматриваемых преступлений.

Сотрудниками органов внутренних дел было выявлено 98 798 краж, совершенных с использованием информационно-телекоммуникационных технологий.

В структуре преступлений в сфере информационных технологий особое место занимают мошенничества (46,4 %), кражи (33,5 %) и деяния в сфере незаконного оборота наркотических средств и психотропных веществ (8,4 %) (табл. 7.1).

Таблица 7.1

Преступления в сфере информационных технологий, 2018–2019 гг.[1]

Статья УК РФ	2018	2019	Прирост, %
110	13	4	–69,2
110.1	18	11	–38,9
137	432	508	+17,6
138	143	180	+25,9
138.1	289	125	–56,7

[1] Ф4 – ЕГС (494). Книга 31. Раздел 11 «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации» // Сборник по России, январь – декабрь 2019 г.

Статья УК РФ	2018	2019	Прирост, %
146	406	332	–18,2
151	1	0	–100,0
151.2	1	0	–100,0
158	32 668	98 798	+202,4
159	90 664	119 903	+32,2
159.3	4 242	16 119	+280,0
159.6	970	687	–29,1
163	1 621	2 090	+28,9
165	11	21	+90,9
171.2	875	842	–3,8
183	90	185	+105,6
187	203	433	+113,3
205.2	169	212	+25,4
222, 222.1	68	56	–17,6
228.1	18 805	24 677	+31,2
228.4	2	10	+400,0
230	5	1	–80,0
234	106	129	+21,7
242	725	972	+34,1
242.1	548	704	+28,5
242.2	195	240	+23,1
272	1 761	2 420	+37,4
273	733	455	–37,9
274	5	4	–20,0
274.1	1	4	+300,0
280	253	257	+1,6
280.1	10	6	–40,0
282	733	12	–98,4

Структурно-динамические изменения вышеуказанных статистических характеристик позволяют сделать вывод о нестабильной

тенденции развития преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Вышеобозначенные тенденции связаны не столько с реальным увеличением, а в отдельных случаях и снижением преступлений, совершенных с использованием информационно-телекоммуникационных технологий, сколько с различными проблемами, возникающими в процессе выявления, расследования и раскрытия данных преступлений, а также с другими существенными негативными факторами, формирующими предмет доказывания.

Интенсификация оперативно-разыскных мероприятий позволила значительно увеличить следственно-судебную перспективу рассматриваемых преступлений. Количественные параметры изменения практики привлечения к уголовной ответственности за преступления, совершенные с использованием информационно-телекоммуникационных технологий, нашли свое естественное закрепление в данных статистического учета и отчетности.

Наибольший удельный вес в структуре преступлений в сфере информационных технологий занимают следующие преступные деяния:

– мошенничество (ст. 159 УК РФ);

– кража (ст. 158 УК РФ);

– незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ);

– мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);

– вымогательство (ст. 163 УК РФ);

– мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

– неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

Представленный анализ позволяет сделать вывод о том, что большинство указанных преступлений совершается путем мошеннических действий и краж. Информатизация общества привела к увеличению и изменению схем мошеннических действий и краж, совершенных с использованием информационно-телекоммуникационных технологий.

Так, согласно сведениям ГИАЦ МВД России, за 2019 г. на территории России зарегистрировано 119 903 преступления, предусмотренных ст. 159 УК РФ (прирост за год – 32,2 %), ст. 159.3 УК РФ – 16 119 преступлений (прирост за год – 280 %), ст. 159.6 УК РФ – 687 (прирост за год – 29,2 %)[1].

По своему механизму, способам совершения и сокрытия эти преступления имеют определенную специфику, характеризуются высоким уровнем латентности и низким уровнем раскрываемости.

Общими предпосылками к распространению преступлений в сфере информационных технологий являются следующие факторы:

– рост количества финансовых операций и сделок, осуществляемых опосредованным контактом (интернет-торговля);

– увеличение доступности и конфиденциальности персональной информации;

– снижение возраста пользователей, участвующих в финансовых сделках;

---

[1] Представить статистические сведения за более ранний период не представилось возможным, поскольку ст.ст. 159.3 и 159.6 были внесены в УК РФ 23 апреля 2018 г. в связи с принятием Федерального закона от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». До этого момента все мошеннические действия, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, квалифицировались по ст. 159 УК РФ.

– стирание границ для перемещения денежных средств, товаров и услуг, вызванное глобализацией и технологизацией;

– увеличение разновидностей форм финансовых ресурсов.

Одной из специфических тенденций проявления мошенничества в сфере информационных технологий является то обстоятельство, что все чаще преступники, в том числе рецидивисты, отбывшие наказание, связанное с лишением свободы, получают от сокамерников-мошенников знания о более легком и безопасном заработке путем совершения хищений в сфере информационных технологий.

Основной проблемой, связанной с раскрытием преступлений указанной категории, является то, что лица, осуществляющие звонки на телефоны потерпевших, как правило, находятся на территории других субъектов Российской Федерации либо в исправительных учреждениях различного типа.

Абонентские номера сотовых операторов, с которых осуществляются звонки потерпевшим, в большинстве случаев зарегистрированы на утерянные паспорта граждан либо были приобретены без предоставления документов, удостоверяющих личность. Поэтому по таким преступлениям сложно установить личность преступника и доказать его причастность к совершению преступлений.

За январь – сентябрь 2020 г. по ст. 159 УК РФ зафиксировано увеличение фактов рассматриваемых преступлений почти в два раза по всем федеральным округам (**прирост – 77,9 %**) по сравнению с аналогичным периодом 2019 г.

Уголовные дела, которые направлены в суд с обвинительным заключением, в среднем направляются в 7,5 % материалов уголовных дел от общего числа зарегистрированных (табл. 7.2).

За январь – сентябрь 2020 г. по сравнению с аналогичным периодом 2019 г. по ст. 159.3 УК РФ в среднем зарегистрирован двукратный рост во всех федеральных округах (**прирост – 119,4 %**): в Уральском федеральном округе – в 3 раза, в Южном – в 2,5 раза, в Дальневосточном – в 2,4 раза.

Таблица 7.2

Преступления, предусмотренные ст. 159 УК РФ, совершенные в сфере информационно-телекоммуникационных технологий, 2018–2019 гг.

Федеральный округ	Зарегистрировано преступлений		Уголовных дел направлено в суд с обвинительным заключением, актом или постановлением	
	2018	2019	2018	2019
Центральный	20 741	28 516	2 148	2 298
Северо-Западный	8 039	10 217	365	489
Северо-Кавказский	3 048	3 978	301	225
Южный	11 857	15 525	703	613
Приволжский	19 255	24 606	1 466	1 540
Уральский	8 973	12 439	840	733
Сибирский	12 198	16 407	1 114	1 332
Дальневосточный	6 266	7 966	510	616
Территории	90 392	119 716	7 450	7 870
Транспорт	272	187	87	170
Всего по России	90 664	119 903	7 537	8 040

Уголовные дела, которые направлены в суд с обвинительным заключением, в среднем направляются в 13,6 % случаев от всех зарегистрированных (табл. 7.3).

Таблица 7.3

Преступления, предусмотренные ст. 159.3 УК РФ, совершенные в сфере информационно-телекоммуникационных технологий, 2018–2019 гг.

Федеральный округ	Зарегистрировано преступлений		Уголовных дел направлено в суд с обвинительным заключением, актом или постановлением	
	2018	2019	2018	2019
Центральный	840	2 451	51	537
Северо-Западный	550	1 935	34	319
Северо-Кавказский	293	632	1	24
Южный	342	1208	17	156
Приволжский	1 197	5 017	108	882
Уральский	227	1 036	63	362
Сибирский	651	2 789	78	429
Дальневосточный	135	995	30	249
Всего по России	4 242	16 119	382	2 958

Уголовные дела, материалы по которым направлены в суд с обвинительным заключением, составляют в среднем 6,7 % от всех зарегистрированных случаев (табл. 7.4).

В общем количестве зарегистрированных мошеннических действий, совершенных с использованием информационно-телекоммуникационных технологий, классические виды составляют бóльшую часть. Мошенничество в сфере телекоммуникаций становится альтернативой традиционному финансовому преступлению с низким уровнем риска.

Таблица 7.4

Преступления, предусмотренные ст. 159.6 УК РФ, совершенные в сфере информационно-телекоммуникационных технологий, 2018–2019 гг.

Федеральный округ	Зарегистрировано преступлений		Уголовных дел направлено в суд с обвинительным заключением, актом или постановлением	
	2018	2019	2018	2019
Центральный	133	81	29	6
Северо-Западный	194	77	0	0
Северо-Кавказский	30	9	1	1
Южный	36	27	1	2
Приволжский	276	321	39	15
Уральский	202	108	3	5
Сибирский	51	35	2	3
Дальневосточный	24	22	1	3
Всего по России	970	687	81	35

При осуществлении преступного замысла интернет-мошенники традиционно используют давно известные предлоги мошеннических действий, совершаемых посредством компьютерных технологий и средств мобильной связи: продажа (покупка) товаров на различных интернет-ресурсах («Авито», «Юла» и др.), в том числе фишинговых, сообщение ложных сведений о выигрыше приза, ложная информация о задержании близких лиц за совершение различных правонарушений.

Самыми распространенными формами кибермошенничества выступают:

1. Фишинг (англ. phishing, от fishing – рыбная ловля) – вид интернет-мошенничества, целью которого является получение

доступа к конфиденциальным данным пользователей: логинам, паролям, PIN-кодам, номерам счетов.

2. Вишинг (vishing, voice + phishing – голосовая рыбная ловля) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей при помощи телефона. Технология вишинга заключается в использовании автонабирателей (war diallers) и возможностей интернет-телефонии (VoIP) для хищения конфиденциальных данных в корыстных целях. Потенциальные жертвы получают на свой электронный адрес сервисные сообщения от имени известных организаций, в которых содержится просьба позвонить на определенный городской номер.

3. Спуфинг, или IP-спуфинг (англ. spoof – обман, имитация) – вид сетевой атаки, при которой хакер внутри организации или за ее пределами выдает себя за санкционированного пользователя. Используется для обхода систем управления доступом на основе IP-адресов, а также для маскировки ложных сайтов под их легальных двойников.

4. Фарминг (англ. pharming, phishing + farming – выращивание) – вид интернет-мошенничества, позволяющий изменять DNS-записи либо записи в файле hosts для проведения скрытой атаки.

Интенсификации практики регистрации преступлений по ст.ст. 159, 159.3, 159.6 УК РФ способствовало принятие постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» в целях обеспечения единообразного применения судами норм уголовного закона об ответственности за мошенничество. Постановлением были четко дифференцированы способы хищения чужого имущества или приобретения права на чужое имущество по ст.ст. 159–159.3, 159.5–159.6 УК РФ.

Также за последние годы сформировалась практика по возбуждению уголовных дел по ст.ст. 159.3, 159.6 УК РФ, были

определены критерии предмета доказывания, что увеличило практику по расследованию и раскрытию преступлений данной направленности.

Статистические данные фиксируют за январь – сентябрь 2020 г. по п. «г» ч. 3 ст. 158 УК РФ («Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств») 121 220 преступлений, за январь – сентябрь 2019 г. – 67 074 преступлений (**прирост – 80,7 %**) (табл. 7.5).

Таблица 7.5

Преступления, предусмотренные ст. 158 УК РФ, совершенные в сфере информационно-телекоммуникационных технологий, 2018–2019 гг.

Федеральный округ	**Зарегистрировано преступлений**		**Уголовных дел направлено в суд с обвинительным заключением, актом или постановлением**	
	2018	**2019**	**2018**	**2019**
Центральный	5 756	24 531	1 071	3 755
Северо-Западный	2 620	9 121	777	2 081
Северо-Кавказский	676	2 507	119	606
Южный	1 929	8 310	371	1 687
Приволжский	8 088	22 969	1 847	4 225
Уральский	3 545	9 216	1 109	1 866
Сибирский	6 918	15 441	1 867	3 445
Дальневосточный	2 981	6 413	904	1 907
Территории	32 528	98 565	8 068	19 618
Транспорт	140	233	73	150
Всего по России	32 668	98 798	8 141	19 768

Значительный удельный вес именно данного вида краж позволяет сделать вывод об активации преступной деятельности

в этом направлении, что связано с перемещением различных способов хищения в сферу информационных технологий.

Кража, совершенная с использованием информационно-телекоммуникационных технологий[1], – это хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Преступные действия в виде кражи могут быть совершены путем:

– взлома и похищения баз данных у различных государственных структур и учреждений;

– «физической кражи» документов, банковских карт или чеков;

– восстановления личных данных с жестких дисков и других электронных носителей информации, не подготовленных перед их утилизацией или продажей;

– кражи или подделки отпечатков пальцев, голоса и прочих биометрических данных;

– получения информации из социальных сетей или других открытых источников;

– заражения устройств вредоносными программами для получения необходимой информации.

Введение подобного рода уголовной ответственности позволило интенсифицировать практику инкриминирования именно по этому специальному виду квалифицированных краж.

---

[1] Понятие «Кража, совершенная с использованием информационно-телекоммуникационных технологий» употребляется нами в контексте Ф4 – ЕГС (494) Книга 31. Раздел 11, где название ст. 158 УК РФ «Кража» предусмотрено в качестве самостоятельного преступления в сфере информационно-телекоммуникационных технологий или в сфере компьютерной информации. Учетная позиция предполагает отнесение данных преступлений к п «г» ч. 3 ст. 158 УК РФ.

Представленные данные позволяют указать средние значения количества уголовных дел, материалы по которым направлены в суд с обвинительным заключением по всем субъектам Российской Федерации – 22,5 % от всех зарегистрированных случаев.

Уголовные дела, материалы которых направлены в суд с обвинительным заключением, в среднем по всем субъектам Российской Федерации составляют 47,2 % от всех зарегистрированных преступных деяний, предусмотренных ст. 228.1 УК РФ. Это наибольший удельный вес материалов уголовных дел, направленных в суд, среди всех преступлений в сфере информационных технологий (табл. 7.6).

Статистические данные за январь – сентябрь 2020 г. по ст. 228.1 УК РФ содержат сведения о 29 580 преступлениях. За такой же период в 2019 г. совершено 17 871 преступление (**прирост – 65,5 %**)[1].

Наибольший рост зафиксирован в Северо-Западном округе – в 3,4 раза, в Северо-Кавказском – в 3,3 раза, в Центральном – в 2,7 раза. **30 %** преступлений, предусмотренных ст. 228.1 УК РФ, приходится на Приволжский федеральный округ.

Незаконный оборот наркотических средств и психотропных веществ на торговых площадках продолжает увеличиваться. Это приводит к увеличению клиентов по сбыту наркотических средств из-за возможности анонимного приобретения.

Такие преступления могут совершаться на значительном расстоянии, включая все большие территории сбыта. Условием, способствующим совершению подобных преступлений, является функционирование различных торговых площадок. Сама площадка внешним видом напоминает форум, где у каждого

[1] Ф4 – ЕГС (494). Книга 31. Раздел 11 «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации» // Сборник по России, январь – декабрь 2019 г., январь – сентябрь 2020 г.

продавца есть своя ветка – «магазин» с описанием доступных товаров, списком контактов и отзывами клиентов.

Таблица 7.6

Преступления, предусмотренные ст. 228.1 УК РФ, совершенные в сфере информационно-телекоммуникационных технологий, 2018–2019 гг.

Федеральный округ	Зарегистрировано преступлений		Уголовных дел направлено в суд с обвинительным заключением, актом или постановлением	
	2018	2019	2018	2019
Центральный	1 527	2 554	612	1 286
Северо-Западный	773	1 393	337	576
Северо-Кавказский	217	470	180	131
Южный	1 386	1 813	324	384
Приволжский	5 708	7 749	2 754	4 032
Уральский	5 139	5 671	2 032	2 125
Сибирский	2 351	2 915	645	760
Дальневосточный	462	600	102	181
Всего по России	18 805	24 677	9 004	11 494

Меняется структура наркопотребления, в ней превалируют синтетические наркотические средства. Формируется вектор на потребление новых синтетических наркотиков – мефедрона и альфа-ПВП. Основные причины – их легкий синтез и низкая цена. Снижается потребление героина: его доля на российском рынке, по оценкам специалистов, составляет 0,3 % от всех потребляемых наркотических веществ.

Одной из распространенных тенденций является использование криптовалют для расчета за покупку наркотиков на крипторынках.

Некоторые криптовалюты предусматривают анонимность: например, для проведения транзакции в биткоинах необходим только номер кошелька.

Сбыт наркотических средств и психотропных веществ все чаще происходит через мессенджеры Viber, WhatsApp и Telegram, социальные сети «Одноклассники», «ВКонтакте», Facebook и Twitter. Особой популярностью пользуются различные системы анонимайзеров, в том числе Tor и VPN. Большинство пользователей Tor-сети приходит в нее ради приобретения запрещенных веществ. Для перевода денежных средств применяются электронные платежи WebMoney, QIWI и «Яндекс.Деньги».

Альтернативные платформы, такие как социальные сети, приложения для обмена мгновенными сообщениями и приложениями для защищенной связи, будут все шире использоваться для содействия распространению незаконных товаров, включая наркотики, в интернет-пространстве.

COVID-19 также выступает одним из факторов развития незаконного оборота наркотиков. Пользователям стало труднее получить определенные виды наркотических средств и психотропных веществ, в связи с этим они могут попытаться получить свои препараты альтернативными методами.

Применение автоматизированных информационных технологий управления и обработки информации, придание значительной юридической силы актам, осуществляемым с помощью компьютерных программ, обусловили и сформировали предпосылки использования этих процессов для совершения преступных действий, в том числе неправомерного доступа к компьютерной информации. Все это повлекло уничтожение, блокирование, модификацию либо копирование информации. Наблюдаемые статистические изменения с момента установления ответственности (норма действует более 20 лет) позволяют сделать вывод о тенденции стабильного роста преступлений, предусмотренных ст. 272 УК РФ. В связи с ролью информации как одного из основных

ресурсов в жизни общества усложняются процессы ее добычи, обработки, хранения и защиты.

Уголовные дела, материалы по которым направлены в суд с обвинительным заключением, в среднем составляют 13,3 % от всех зарегистрированных случаев (табл. 7.7).

Таблица 7.7

Преступления, предусмотренные ст. 272 УК РФ, совершенные в сфере информационно-телекоммуникационных технологий, 2018–2019 гг.

Федеральный округ	**Зарегистрировано преступлений**		**Уголовных дел направлено в суд с обвинительным заключением, актом или постановлением**	
	2018	**2019**	**2018**	**2019**
Центральный	236	285	54	30
Северо-Западный	244	307	20	9
Северо-Кавказский	27	56	3	15
Южный	131	202	11	24
Приволжский	730	1 036	91	90
Уральский	130	215	16	19
Сибирский	147	230	28	110
Дальневосточный	91	83	6	12
Территории	1 737	2 416	229	309
Транспорт	24	4	15	2
Всего по России	1 761	2 420	244	311

Противозаконные требования о передаче денежных средств, имущества, иных ценностей все чаще стали выдвигаться в сфере информационно-телекоммуникационных технологий. Преимущественно целями шантажа являются:

– вымогательство денег или иных материальных благ;

– месть личного характера;

– принуждение к совершению юридических или социальных действий;

– иные действия.

В большинстве случаев злоумышленники угрожают пользователям осуществлением следующих действий: распространением личных данных коммерческого или интимного характера; ложным доносом в полицию; взломом личных страниц в социальных сетях и почтовых серверах; заражением компьютера пользователя вредоносными программами; причинением вреда или физического насилия.

Таблица 7.8

Преступления, предусмотренные ст. 163 УК РФ, совершенные в сфере информационно-телекоммуникационных технологий, 2018–2019 гг.

Федеральный округ	Зарегистрировано преступлений		Уголовных дел направлено в суд с обвинительным заключением, актом или постановлением	
	2018	2019	2018	2019
Центральный	352	455	49	36
Северо-Западный	179	235	5	20
Северо-Кавказский	62	55	13	19
Южный	88	163	11	11
Приволжский	521	613	43	39
Уральский	190	284	32	28
Сибирский	185	224	15	21
Дальневосточный	40	56	1	29
Всего по России	1 621	2 090	169	203

Представленные статистические данные позволяют сделать вывод о стабильном росте числа вымогательств в сфере информационно-телекоммуникационных технологий. Уголовные дела, материалы по которым направлены в суд с обвинительным заключением, в среднем составляют 13,3 % от всех зарегистрированных случаев (табл. 7.8).

Другой тревожной тенденцией в преступной деятельности остаются незаконные изготовление и оборот порнографических материалов или предметов, в том числе материалов или предметов с порнографическими изображениями несовершеннолетних.

Произошла регистрация новых преступных деяний в киберпространстве, таких как ст. 242 УК РФ («Незаконные изготовление и оборот порнографических материалов или предметов»), ст. 242.1 УК РФ («Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»).

Преступники пытаются воспользоваться эмоционально уязвимыми, изолированными несовершеннолетними в целях сексуального принуждения и вымогательства. Подростки с неконтролируемым интернет-доступом будут все более и более уязвимы перед лицом правонарушителей в результате таких онлайн-действий, как онлайн-игры, использование групп чатов в приложениях, попытки фишинга по электронной почте, нежелательные контакты в социальных сетях и др.[1]

Статистические данные ГИАЦ МВД России демонстрируют следующие количественные характеристики лиц, совершающих преступления в сфере информационных технологий: в 2018 г.

[1] Porn and Predators: Activists Warn of Internet Dangers for Kids During Coronavirus Crisis // Daily Caller. URL: https://dailycaller.com/2020/03/28/porn-predators-internet-coronaviruschildren ; Report: WhatsApp has seen a 40 % increase in usage due to COVID-19 pandemic // TechCrunch. URL: https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19pandemic ; ‘Zoom-bombing’ on the rise: Hijackers invade videoconferences for work, school, FBI says // The Mercury News. – URL: https://www.mercurynews.com/2020/03/31/coronavirus-zoom-bombing-hijackers-videoconferences.

выявлено 24 002 лица, в 2019 г. – 44 158, совершивших преступления с использованием информационно-телекоммуникационных технологий, из которых 10 752 – женщины. В зависимости от возраста преступника выявленных лиц можно подразделить на следующие категории: 14–15 лет (463 преступника), 16–17 лет (1 705), 18–24 (10 868), 25–29 (9 181), 30–49 (19 981), 50 и старше (1 960)[1].

За январь – сентябрь 2020 г. выявлено 47 569 лиц, совершивших преступления в сфере информационных технологий (за тот же период 2019 г. – 32 450, **прирост – 46,5 %**)[2].

Увеличению правоприменительной практики по преступлениям в сфере информационных технологий способствует ряд обстоятельств:

1. Социально-экономические: низкий уровень жизни населения и возможность получения сверхдоходов мошенническим способом, путем совершения краж; увеличивающийся разрыв между богатым слоем населения и бедным; высокий уровень цен на продукты и иные необходимые товары; сокращение количества рабочих мест и т. д.[3]

2. Виктимологические: отсутствие у граждан базовых знаний об интернет-безопасности при покупке, продаже товаров; легкомысленное отношение населения к доводимой профилактической информации о популярных способах мошеннических действий и методиках противодействия им.

---

[1] Статистические сведения Центра статистической информации ГИАЦ МВД России. Режим доступа: форма «2-ЕГС» (492) за январь – декабрь 2019 г. Раздел: 1. Код: 1200.

[2] Статистические сведения Центра статистической информации ГИАЦ МВД России. Режим доступа: форма «2-ЕГС» (492) за январь – сентябрь 2020 г.

[3] Молчанова Т. В., Аксенов В. А. Факторы, обуславливающие мошенничество, совершенное с использованием информационно-телекоммуникационных технологий // Вестник экономической безопасности. 2020. № 2. С. 93–98.

3. Технические: несовершенство системы защиты онлайн-банкинга в кредитных организациях от применения методик социальной инженерии в отношении клиентов; отсутствие надлежащей модерации интернет-ресурсов, осуществляющих услуги по размещению объявлений (например, «Авито», «Юла»), за идентификацией пользователей при регистрации на сайте; наличие в свободном доступе средств интернет-анонимизации (виртуальная частная сеть, прокси-сервера, Tor-браузер); возможность осуществлять звонки с использованием услуг IP-телефонии, в том числе с подменой виртуальных номеров и голоса; использование различных мессенджеров по обмену информацией – как в текстовой, так и в звуковой форме; доступность приобретения симкарт, банковских карт, мобильных телефонов, логинов и паролей от взломанных аккаунтов в социальных сетях, принадлежащих третьим лицам.

Как и в случае со многими преступлениями, совершаемыми не в интернете, денежные средства выступают основным мотиватором для многих преступлений в сфере информационных технологий. Опасность наступления последствий менее очевидна, когда преступник прячется за Сетью, ощущение низкого уровня риска и высокого финансового вознаграждения побуждает многих киберпреступников участвовать в создании вредоносных программ, фишинге, краже личных данных и мошеннических атаках с использованием методов социальной инженерии для завладения денежными средствами жертвы.

Безусловно, интенсивность использования отразилась на современных тенденциях преступности в сфере информационных технологий. Это выразилось в прогрессировании организованного характера совершения преступлений, расширении сферы преступных действий, усложнении и модификации применяемых преступных схем, росте числа мошеннических действий, связанных с использованием электронной подписи при оказании государственных услуг, регистрации сделок, имущества и иных действий.

Одной из негативных тенденций является сохранение значительной доли участия в совершении мошеннических действий лиц, отбывающих наказание в исправительных учреждениях различного типа. На территории исправительных учреждений не обеспечены должные меры по ограничению использования мобильной связи в целях осуществления обмана держателей вкладов в банках с использованием аналогов специальных банковских программ и услуг.

Прогнозируется рост преступлений с использованием информационных технологий террористическими и экстремистскими организациями. Основные цели здесь – вербовка граждан и распространение экстремистских взглядов, убеждений. В связи с этим одним из приоритетных направлений деятельности в рамках информационного противодействия вербовочной деятельности террористических организаций должен стать мониторинг информационной активности вовлечения членов террористических и экстремистских организаций с использованием больших данных (big data), блокчейна (blockchain) и дата-майнига (data mining).

Продолжится рост преступлений в сфере информационных технологий, связанных с незаконным оборотом огнестрельного оружия, его основных частей, боеприпасов, взрывчатых веществ или взрывных устройств, их хищением различными способами и вымогательством.

Сохранится тенденция роста незаконного оборота наркотических средств, психотропных веществ или их аналогов, растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, прекурсоров наркотических средств или психотропных веществ, а также растений, содержащих прекурсоры наркотических средств или психотропных веществ.

Важным фактором выступает уровень цифровой грамотности пользователей, который в России ежегодно увеличивается,

однако недостаточными темпами: только 27 % россиян обладает высоким уровнем цифровой грамотности[1]. Цифровая безопасность показывает умения россиян оценивать риски социальной инженерии и онлайн-мошенничества при работе в цифровом пространстве, знание мер по обеспечению безопасности персональных данных, а также понимание негативного влияния, которое цифровые устройства оказывают на окружающую среду, физическое и психическое здоровье человека.

Представленное описание статистического измерения преступлений в сфере информационных технологий, а также отдельные проблемы практики выявления и расследования подобного рода преступлений позволяют утверждать, что использовать только их для оценки, прогнозирования и предупреждения рассматриваемого вида преступности не представляется объективным. Правоприменительная практика находится только в процессе своего формирования.

С учетом динамики развития преступлений данной категории прогнозируется дальнейший рост в связи с внедрением в преступные схемы новых методик социальной инженерии и применением новейших информационных технологий (средства IP-телефонии, SIM box, криптовалюта и др.).

§ 7.2. Предупреждение преступлений в сфере информационных технологий

Несмотря на все предпринимаемые усилия по противодействию киберпреступности, улучшения ситуации в данной сфере не наблюдается.

[1] Цифровая грамотность россиян: исследование, 2020 г. // НАФИ. URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020.

В 2019 г. практически каждое седьмое преступление было совершено в сфере информационно-коммуникационных технологий или с использованием компьютерной информации, в том числе с применением пластиковых банковских карт, компьютерной техники, интернета и средств мобильной связи.

Особо выделим финансово-кредитную сферу отношений – одну из наиболее атакуемых киберпреступниками. На протяжении последних нескольких лет отмечается устойчивый рост преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. На сегодняшний день киберпреступность в финансово-кредитной сфере превратилась в организованный и достаточно прибыльный криминальный бизнес.

По данным Банка России, в 2019 г. в финансово-кредитной сфере объем всех операций, совершенных без согласия клиентов (физических и юридических лиц) с использованием ЭСП, составил 6,4 млрд руб.

Активное внедрение и использование российскими кредитными организациями технологий дистанционного банковского обслуживания клиентов сопровождается возникновением новых рисков и угроз для деятельности кредитных организаций, включая криминальные. Во-первых, это хакерские атаки на системы дистанционного банковского обслуживания; во-вторых, активное использование методов социальной инженерии, в результате применения которых владелец банковского счета, будучи введенным в заблуждение, либо сам переводит средства со своего счета на счет преступников, либо передает конфиденциальную информацию (свои персональные данные, данные банковской карты, пароли, коды), необходимую для получения доступа к счету.

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России (ФинЦЕРТ Банка России) в 2015–2018 гг. публиковал ежегодные обзоры несанкционированных переводов денежных средств (обзоры несанкционированных

переводов денежных средств с использованием платежных карт, несанкционированных операций со счетов юридических лиц, сведения об инцидентах, произошедших при эксплуатации операторами по переводу денежных средств и операторами услуг платежной инфраструктуры объектов информационной инфраструктуры)[1]. Начиная с 2019 г. ФинЦЕРТ Банка России публикует обзор операций, совершенных без согласия клиентов финансовых организаций[2].

На основе ежегодных обзоров несанкционированных переводов денежных средств проанализируем тенденции изменения объема несанкционированных операций с использованием платежных карт (рис. 7.2) и количества несанкционированных операций с использованием платежных карт (рис. 7.3).

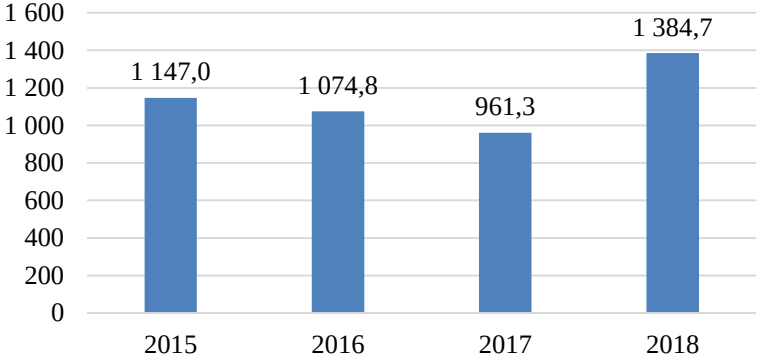


Рис. 7.2. Объем несанкционированных операций с использованием платежных карт, 2015–2018 гг., млн руб.

[1] ФинЦЕРТ // Банк России. URL: https://cbr.ru/information_security/fincert .

[2] Рост показателей количества и объема хищений в 2019 г. произошел ввиду изменения в 2018 г. формы отчетности 0403203, а также запуска АСОИ ФинЦЕРТ и АС «Фид-Антифрод», что позволило повысить выявляемость операций без согласия клиентов. По нашему представлению, показатели за 2015–2018 гг. и 2019 г. не являются полностью сопоставимыми.

Объем несанкционированных переводов денежных средств с использованием платежных карт снижался в 2015–2017 гг., однако в 2018 г. возрос до 1 384,7 млн руб. (+44 % по сравнению с 2017 г.). В 2019 г. объем всех операций, совершенных без согласия клиентов – физических лиц с использованием ЭСП, составил 5 723,5 млн руб.

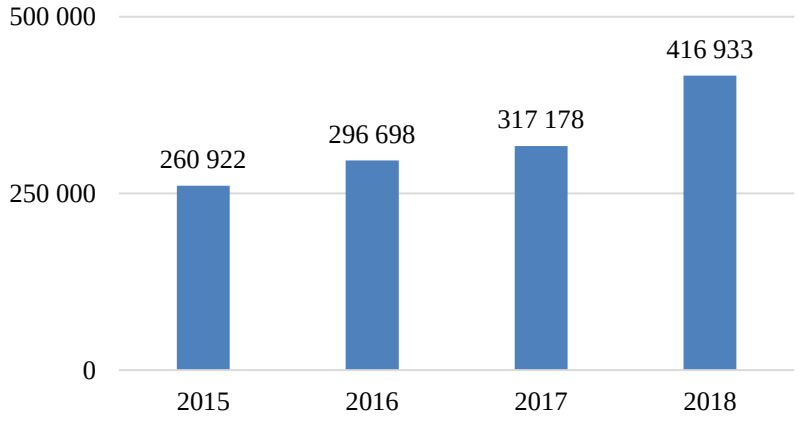


Рис. 7.3. Количество несанкционированных операций с использованием платежных карт, 2015–2018 гг., единиц

Количество несанкционированных операций с использованием платежных карт ежегодно увеличивается, а в 2019 г. составило 571 957 операций.

Жертвами киберпреступников становятся также и юридические лица. Проанализируем динамику объема и количества несанкционированных операций со счетов юридических лиц[1]

[1] Согласно ежегодным обзорам несанкционированных переводов денежных средств, под несанкционированными операциями со счетов юридических лиц понимаются события, связанные с хищением (покушением на хищение) денежных средств со счета юридического лица с использованием систем ДБО.

за 2015–2018 гг. (рис. 7.4–7.5), а также объем и количество операций без согласия клиентов юридических лиц[1] за 2019 г.

На протяжении 2015–2018 гг. объем хищений денежных средств у юридических лиц постоянно снижался, а в 2019 г. составил 701 млн руб. – почти вдвое меньше, чем в 2018 г.

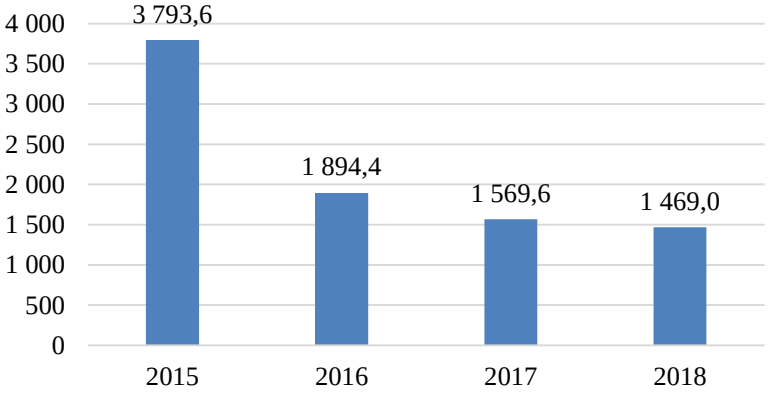


Рис. 7.4. Объем несанкционированных операций со счетов юридических лиц, 2015–2018 гг., млн руб.

В 2016 г. наблюдалось незначительное снижение количества несанкционированных операций со счетов юридических лиц по сравнению с 2015 г., однако уже в 2017 г. показатель увеличился на 17,2 %, а в 2018 г. – более чем в семь раз. В 2019 г. юридические лица сообщили о 4 609 операциях, осуществленных без согласия клиента.

[1] Согласно обзору операций, совершенных без согласия клиентов финансовых организаций, под операциями без согласия клиентов со счетов юридических лиц понимаются события, по которым клиенты сообщили о хищениях средств в результате несанкционированного доступа к системам (средствам) дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей и лиц, занимающихся частной практикой, включая системы (средства), используемые для переводов денежных средств по корреспондентским счетам юридических лиц.

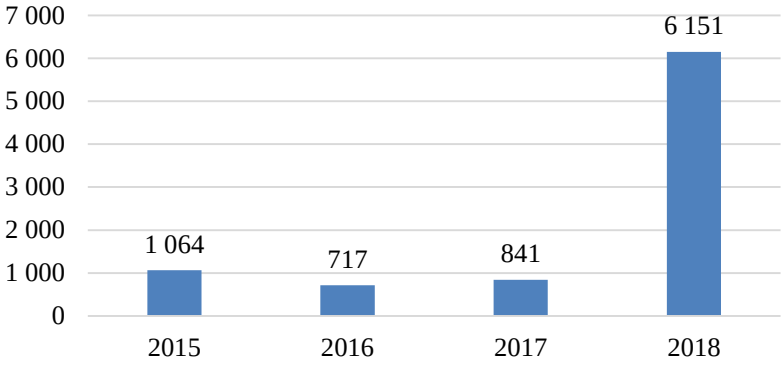


Рис. 7.5. Количество несанкционированных операций со счетов юридических лиц, 2015–2018 гг., единиц

Подобное снижение можно объяснить активными действиями коммерческих организаций по обеспечению информационной безопасности в условиях активного использования информационных технологий.

В качестве основных причин несанкционированных операций с использованием платежных карт указываются:

– использование ЭСП без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности;

– нарушение клиентом порядка использования ЭСП;

– побуждение владельца ЭСП к совершению операции путем обмана и злоупотребления доверием;

– воздействие вредоносного кода.

Основными причинами несанкционированных операций со счетов юридических лиц выступают нарушение порядка использования ЭСП и использование ЭСП без согласия клиента. С учетом того, что юридические лица в основном осуществляют операции через системы дистанционного банковского обслуживания со стационарных компьютеров, причины в большинстве случаев могут быть сведены к воздействию вредоносного кода.

Как отмечают кредитные организации, значительный объем хищений средств со счетов клиентов банков обусловлен относительной простотой их совершения при помощи методов социальной инженерии, использование которых, как правило, не предполагает специальных технических знаний и технических средств у преступников.

Объем хищений и покушений на хищения средств со счетов клиентов банков, совершаемых методом социальной инженерии, непрерывно увеличивается и в настоящее время составляет до 69 % от общего числа подобных преступлений.

Особенностью таких хищений является подтверждение правомерности совершения операции владельцем счета, который находится под влиянием злоумышленников, – даже в случаях, когда служба банка по противодействию кибермошенничеству в системе дистанционного банковского обслуживания определяет операции как подозрительные при осуществлении фрод-мониторинга.

Социальная инженерия активно используется хакерами и при атаках клиента банка с помощью вредоносного программного обеспечения, позволяя получить удаленный доступ к устройству клиента.

Учитывая особенности киберпреступности, становится очевидным, что эффективно противодействовать ей возможно лишь на международном уровне, так как усилий отдельных государств недостаточно. Каждое государство имеет свою собственную правовую систему с различными законами, в основе которых лежат социальные ценности и нормы, складывавшиеся годами, поддерживаемые традициями и обеспеченные политической властью. Мировое сообщество понимает необходимость активного сотрудничества по вопросам обеспечения безопасности киберпространства посредством подписания ряда международных соглашений.

Руководители транснациональных технологических корпораций призывают государства и международные регуляторы активнее участвовать в управлении глобальным киберпространством, считая необходимым как можно быстрее выработать международные правила и стандарты, создать единый профильный орган регулирования. Злоумышленники все чаще атакуют не только корпорации и физических лиц, но и социально значимые объекты. Для таких случаев нужны превентивные меры, возможность прогнозировать угрозы на основе имеющегося опыта и создавать устойчивые механизмы информационного обмена. Борьба с интернет-офшорами также требует совместных усилий: преступники должны понимать, что они не уйдут от ответственности даже сменив домен, поскольку нарушают международные правила.

Киберпреступность – серьезная проблема, решение которой предполагает развитие и государственно-частного партнерства, причем не только на уровне правительств, но и на уровне правоохранительных органов разных стран. Например, международным судам нужна помощь в формировании понятных и открытых стандартов оценки электронных доказательств для борьбы с их фальсификацией.

Сегодня созданы и действуют международные организации, основной целью которых является обеспечение кибербезопасности, в том числе противодействие киберпреступности.

Международное многостороннее партнерство против киберугроз (IMPACT) – исполнительный орган в области кибербезопасности специализированного учреждения ООН по вопросам информационно-телекоммуникационных технологий – Международного союза электросвязи (МСЭ).

IMPACT объединяет правительства, академические организации и экспертов отрасли в целях повышения способности глобального сообщества решать проблемы, связанные с информационной безопасностью. Партнерство IMPACT является опе-

ративной базой для реализации Глобальной программы кибербезопасности Международного союза электросвязи. IMPACT обеспечивает 193 государствам-членам доступ к специальным знаниям, средствам и ресурсам для эффективного устранения киберугроз, а также оказывает учреждениям ООН помощь в защите их инфраструктур информационно-телекоммуникационных технологий.

Международный альянс обеспечения кибербезопасности (ICSPA) объединяет правительства, частные компании и правоохранительные органы для борьбы с киберпреступностью и обеспечения международного обмена опытом.

Будучи крупнейшей международной полицейской организацией, Интерпол также предпринял шаги по оказанию практического содействия правоохранительным органам государств-членов в выявлении и раскрытии трансграничных преступлений, совершаемых в сфере использования информационно-телекоммуникационных технологий. В Сингапуре создан Международный центр Интерпола по инновациям, разработаны и внедрены новые сервисы, утверждена стратегия противодействия киберпреступности.

Деятельность международных организаций направлена на решения следующих задач:

1. Выработка единых международных стандартов кибердеяний, подлежащих криминализации.

2. Формирование единой терминологии и понятийного аппарата.

3. Оказание консультационной помощи при принятии соответствующих уголовно-правовых норм на национальном уровне[1].

---

[1] Мороз Н. О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий // Вестник Полоцкого государственного университета. Серия D: Экономические и юридические науки. 2011. № 14. С. 147.

В 2019 г. Генассамблея ООН приняла российскую резолюцию о противодействии использованию информационно-коммуникационных технологий в преступных целях и создании рабочей группы по международной информационной безопасности.

Тем не менее, несмотря на всю важность этого процесса, уровень участия государств в международном правотворчестве по вопросам кибербезопасности и противодействию киберпреступности остается низким.

Указом Президента Российской Федерации от 12 декабря 2014 г. № 1274 была принята Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в которой была представлена государственная Система обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА). Эта система представляет собой единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (подразделения ФСБ России). Кроме того, Концепция предполагает создание системы специальных центров по обеспечению кибербезопасности, включающей главный и региональные центры, а также центры органов государственной власти России и субъектов Российской Федерации.

В 2015 г. Банком России по поручению Совета Безопасности Российской Федерации был организован Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ), задачами которого является сбор сведений о кибератаках на банки и их клиентов, о потенциальных киберугрозах, а также передача этой информации финансовым учреждениям.

Руководства банков совместно анализируют сценарии кибератак, обмениваются индикаторами компрометации, телефонами и номерами карт злоумышленников. Это помогает выявить и пресечь такие высоколатентные преступления, как мелкие хищения денежных средств, совершаемые посредством использования информационно-телекоммуникационных технологий. Жертвы преступлений в случае хищений небольших сумм денег, как правило, не сообщают об этом правоохранительным органам. Преступники активно пользуются этим, ставя целью получение значительных сумм денег путем совершения мелких хищений у большого количества лиц.

Деятельность органов внутренних дел также направлена на выявление, раскрытие и расследование преступлений, совершаемых в киберсреде. В оперативных подразделениях, а также в следствии и дознании как на федеральном, так и региональном уровне созданы специализированные подразделения по борьбе с киберпреступностью. Трудности процесса становления подразделений связаны не только с организационно-штатным, кадровым и материально-техническим обеспечением их деятельности, но и со спецификой раскрытия и расследования преступлений в кибесреде.

На заседании коллегии МВД России в ноябре 2019 г. совместно с представителями Банка России, Росфинмониторинга, Роскомнадзора и крупнейших банковских структур были обсуждены и намечены конкретные меры по совместному противодействию преступным деяниям в данной сфере.

Выделим приоритетные направления деятельности органов внутренних дел по предупреждению преступлений в сфере информационных технологий:

1. Одна из главных мер в предупреждении рассматриваемых преступлений – интернет-мониторинг в целях выявления и своевременной блокировки опасного контента (интернет-пирамиды (хайп-проекты), фишинговые сайты, сайты, размещающие

экстремистские, порнографические материалы, онлайн-казино и т. п.). Особое внимание следует обратить на внедрение ПАО «Сбербанк» антифрод-системы в иные финансово-кредитные организации, что обеспечивает временную блокировку счета в случае возникновения сомнений у специалиста в правомерности перевода денежных средств до момента подтверждения собственником.

В целях оперативной блокировки сайтов, мошеннических колл-центров, номеров телефонов, с использованием которых осуществляются мошеннические действия, необходимо разработать и внедрить механизмы взаимодействия органов внутренних дел с другими правоохранительными органами, органами государственной власти и коммерческими организациями.

2. В целях профилактики преступлений, совершаемых в сфере информационных технологий, МВД России необходимо проанализировать актуальность использования рассылки писем гражданам с официального почтового ящика МВД России. Подобная рассылка была бы посвящена предупреждению существующих угроз, в ней демонстрировались бы материалы о современных видах, способах хищений, совершаемых злоумышленниками. Подобного рода информацию необходимо также размещать в самостоятельном разделе официального сайта МВД России, в том числе на официальных сайтах ведомства в субъектах Российской Федерации.

3. Во взаимодействии со средствами массовой информации органам внутренних дел следует информировать население о способах совершения преступлений в сфере компьютерной информации и преступлений, в том числе посредством ЭСП. Задачей здесь выступает формирование культуры личной информационной безопасности (правила хранения данных, периодичность и случаи смены паролей, программы родительского контроля за виртуальной деятельностью несовершеннолетних и т. п.).

4. В целях организации эффективной работы в процессе выявления, раскрытия и расследования преступлений на службу в органы внутренних дел необходимо привлекать лиц, обладающих специальными познаниями и навыками, имеющих образование в сфере информационной безопасности. Необходимо осуществлять подготовку таких специалистов и в образовательных организациях системы МВД России. Кроме того, следует осуществлять переподготовку и повышение квалификации работающих сотрудников органов внутренних дел по проблемам противодействия преступности в сфере информационных технологий.

5. Требуется решение вопроса о возможном изменении форм статической отчетности по преступлениям, совершенным с использованием информационно-телекоммуникационных технологий, с учетом проведения соответствующими подразделениями МВД России мониторинга и анализа формирования подобного рода сведений.

6. Необходимо интенсифицировать практику привлечения коммерческих организаций и IT-компаний для взаимодействия с органами внутренних дел посредством совершенствования системы передачи информации (баз данных) и иных сведений.

7. На основе анализа формирующейся следственной и судебной практики следует своевременно (с учетом изменения видов и способов совершения преступлений) готовить методические рекомендации по выявлению, раскрытию и расследованию преступлений, совершаемых в сфере информационных технологий.

8. Стоит рассмотреть возможность подготовки предложений, направленных на ужесточение ответственности за незаконное разглашение или использование личных данных без согласия их владельца, совершенное лицом, которому она была доверена или стала известна по службе или работе.

9. Необходимо повысить техническую оснащенность органов внутренних дел. Это позволит своевременно реагировать на

сообщения об информационных угрозах, пресекать незаконные действия, выявлять их источник и обеспечивать привлечение виновных к ответственности.

10. Акцентировать внимание следует на такие виды противоправных деяний, как организованная преступность, экстремистская деятельность, террористическая деятельность, незаконный оборот наркотиков, изготовление порнографических материалов, сексуальная эксплуатация и т. д. Указанные виды преступности формируют в том числе правоприменительную практику преступлений в сфере информационных технологий.

11. Для приведения к единообразию правоприменительной практики, повышения качества предварительного расследования преступлений в сфере информационных технологий стоит рассмотреть вопрос об обращении с предложением о закреплении в Пленуме Верховного Суда Российской Федерации разъяснений, касающихся особенностей толкования и применения правовых норм, предусматривающих ответственность за их совершение.

12. Во взаимодействии с подразделениями по делам несовершеннолетних, образовательными организациями, средствами массовой информации необходимо призывать родителей проявлять бдительность в отношении контента, доступного несовершеннолетним, оберегать детей от информации, которая может причинить им вред, негативно повлиять на их развитие.

13. Обязательными видятся обмен информацией и организация работы подразделений ФСИН России и ФСБ России в местах отбывания наказания на региональном и федеральном уровне при выявлении лиц, совершающих мошеннические или иные противоправные действия, связанные с информационно-телекоммуникационной сферой, а также установление технических средств противодействия сигналам сотовой связи (организация технической блокады).

14. Необходимо активизировать проведение углубленных виктимологических и криминологических исследований киберпреступности, направленных на выявление объективных закономерностей, детерминант киберпреступности, характеристик отдельных типов личности киберпреступников, а также различных аспектов обеспечения кибербезопасности.

15. В рамках развития международного сотрудничества в процессе предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере информационных технологий необходимо разработать и закрепить в соответствующих документах механизм взаимодействия органов внутренних дел с правоохранительными органами иностранных государств при осуществлении данной деятельности.

Успешность противодействия киберпреступлениям во многом зависит от возможности быстро идентифицировать кибератаку. Именно поэтому необходимы технологии, в том числе использующие искусственный интеллект, которые помогут быстро зафиксировать взлом и отреагировать на внедрение.

Пользователь – это самое слабое звено в цепочке обеспечения киберзащиты организации и ее клиентов. В последнее время принципиально изменился вектор кибератак: если раньше они были нацелены на банки и коммерческие организации, то теперь – на физических лиц. В 2019 г. более 80 % атак на клиентов банков совершалось с помощью социальной инженерии (обзвоны, опросы, мошенничество в программах лояльности). До недавнего времени преступники в основном выбирали в качестве мишени пожилых людей, в 2019 г. их фокус атак сместился на 25–30-летних.

Компания Group-IB, занимающаяся расследованием информационных преступлений, отмечает необходимость соблюдения правил технической самозащиты для обеспечения собственной безопасности. Компанией разработаны специальные памятки для предотвращения возможности использования информации кибермошенниками. Перечислены действия

пользователей, повышающие степень защиты от кибератак и киберпреступлений[1]:

1. Использование лицензированных компьютерных программ и антивирусных софтов.

2. Использование электронного почтового адреса по конкретному назначению – для регистрации на сайтах, оплаты услуг, передачи важной информации.

3. Открытие вложений только от известных отправителей. При любых сомнениях необходимо связаться с отправителем иным способом.

4. Проверка вложения на наличие вирусов.

5. Нежелательность указания в полученных по электронной почте формах и анкетах личных данных, так как их безопасную передачу могут гарантировать только защищенные сайты.

6. Проверка запросов персональных данных из деловых и финансовых структур путем обращения в эти структуры по контактам, указанным на официальном сайте, но не в электронном письме.

7. Понимание, что при общении с клиентами банки не осуществляют массовую рассылку.

8. Понимание, что требования немедленных действий в чрезвычайных ситуациях с высокой степенью вероятности являются мошенничеством. Преступники вызывают ощущение тревоги, чтобы заставить пользователя действовать в критической ситуации быстро и неосмотрительно.

9. Выпуск дополнительной карты для оплаты товаров в интернете.

---

[1] 11 правил сетевой безопасности: как защититься от кибермошенников // Милосердие.ru. URL: https://www.miloserdie.ru/article/11-pravil-setevoj-gigieny-kak-zashhititsya-ot-kiberprestupnosti.

10. Использование незараженного устройства при взломе страницы после загрузки файла, выполнение процедуры восстановления пароля со сменой учетных данных во всех сервисах, где они совпадали со скомпрометированными.

11. Отказ от взаимодействия с файлами, запрашивающими использование компонентов ActiveX в браузере Internet Explorer. Эти файлы позволяют скриптам, выполняющимся в контексте браузера, осуществлять доступ к объектам ОС, в том числе загружать на нее исполняемые файлы, которые с высокой вероятностью могут оказаться вредоносными объектами и запускать их.

Человек не может справиться с растущим объемом киберугроз, которые обычно предшествуют совершению киберпреступлений, поэтому для этих целей постепенно внедряется искусственный интеллект. Области применения искусственного интеллекта в обеспечении кибербезопасности и борьбе с киберпреступностью связаны с анализом поведения пользователей или систем и выявлением отклонений от заданного образца. Искусственный интеллект используется в системах фрод-мониторинга, позволяющих отслеживать и блокировать мошеннические транзакции на основе анализа. При этом в руках злоумышленника искусственный интеллект может стать средством совершения преступлений, поэтому широкое распространение данных технологий несет в себе и потенциальные риски, которые необходимо учитывать.

Повышение степени защищенности сетей и устройств, информационно-телекоммуникационных технологий неизбежно приведет и к увеличению стоимости кибератак, что сделает их невыгодными для преступников. Добиться этого можно следующими способами:

– сканировать клиентские устройства и требовать улучшения их безопасности;

– отправлять уведомления хостингам, которые используют киберпреступники;

– распространять доказательства атрибуции атак;

– блокировать трафик, идущий от атакующего.

Наиболее перспективным направлением повышения защищенности информационно-телекоммуникационных устройств является использование биометрических технологий, которое получит дальнейшее распространение по следующим направлениям:

– идентификация и аутентификация при доступе к определенным системам;

– идентификация сотрудников (сбор информации, поиск инсайдеров, верификация нарушений со стороны персонала).

Преступления в сфере информационных технологий являются одним из наиболее сложных вызовов нынешнего века. Решить эту проблему на уровне отдельных стран не получится: географически распределенные преступные группы порой располагаются на разных континентах и подпадают под юрисдикцию целого ряда государств, которые имеют разный уровень технологического развития и зрелости правовой базы в этой области. Кроме того, необходимо объединение усилий всех участников, заинтересованных в противодействии киберугрозам, и на национальном уровне: органов государственной власти и местного самоуправления, правоохранительных органов, предпринимательской среды, общественных организаций, исследовательских структур и граждан.

ГЛАВА 8. Актуальные проблемы организации деятельности органов внутренних дел по противодействию преступлениям в сфере информационных технологий (с учетом зарубежного опыта)

Киберпреступность – всемирное явление: цифровые преступления не знают границ и могут совершаться из любой точки планеты. Каждый час во всем мире совершается около 50 тыс. информационных и цифровых преступлений, больше всего противоправных посягательств совершается в США, на которые приходится около 23 % всех деяний, затем следуют Китай (9 %), Германия и Великобритания (по 8 %).

Предполагаемая стоимость ущерба, причиненного хакерами, вредоносными программами и нарушениями данных, по прогнозам достигнет 6 трлн $ с 2020 по 2021 г. Более 92 % вредоносных программ доставляется по электронной почте.

Особое волнение вызывают проблемы, с которыми сталкиваются органы внутренних дел при исполнении своих полномочий и расследовании совершенных преступных посягательств. В частности, повсеместное развитие цифровых технологий приводит к тому, что правоохранительные органы всего мира сталкиваются с проблемами осуществления своей деятельности в условиях повсеместной цифровизации.

Первостепенная проблема всех правоохранительных систем в борьбе с преступлениями в сфере информационных технологий заключается в том, что преступники быстрее адаптируются к происходящим изменениям, тогда как в правоохранительных органах при высоком среднем возрасте сотрудников наблюдается неспособность использовать передовые технические разработки.

По состоянию на 2019 г. преступники в возрасте 16–30 лет составляют 35 % от общего количества лиц, совершивших преступные деяния. Между тем в сфере преступлений, связанных с цифровыми и информационно-телекоммуникационными технологиями, доля молодых преступников (16–35 лет) составляет практически 90 %. Средний возраст сотрудников правоохранительных органов – 35–40 лет, что само по себе не говорит об их неспособности раскрывать киберпреступления, однако может свидетельствовать о низком уровне знаний именно в сфере цифровых технологий.

Дополнительной проблемой, которая касается развивающихся стран, выступает недостаточно развитая материальная база правоохранительных органов. Особенно это заметно в регионах, которые фактически не способны обеспечить возможность расследования и раскрытия киберпреступлений. Сюда же возможно отнести и общее снижение численности сотрудников, что создает повышенную нагрузку на должностных лиц и в некоторых ситуациях не позволяет заниматься сложными информационными преступлениями.

Другая проблема – в различиях национальных законодательств: так, в Германии, Англии и Франции ответственность за некоторые категории цифровых преступлений варьируется от двух месяцев до двух лет, в США может достигать 10 лет тюремного заключения, а в ряде стран Южной Америки ответственность отсутствует вовсе. Сюда же можно добавить, например, и международные офшорные зоны, которые способствуют легализации доходов, полученных посредством совершения цифровых преступных посягательств. Вместе с тем основной международный правовой акт в сфере борьбы с цифровой преступностью датируется 2001 г. По сути, регулирование преступлений в сфере информационных технологий отдано на откуп национальным законодательствам, что представляется в корне неверным.

Наиболее совершенным в вопросе уголовно-правового противодействия посягательствам в указанной сфере является законодательство США. В нем криминализирован широкий спектр деяний, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий: мошенничество, совершаемое с использованием ЭСП, новых методов и услуг, а также создание, распространение и иные манипуляции с электронными средствами доступа, и преступления, связанные с «кражей личности». Конструкция юридических норм американского законодательства позволяет привлекать к ответственности за противоправные деяния в финансовой сфере с использованием новых, еще не получивших широкого распространения информационно-телекоммуникационных технологий.

В большинстве стран заметны две тенденции – ужесточение ответственности за противоправные посягательства в сфере информационных технологий и непрерывная реформация норм уголовного законодательства как реагирование на возникающие угрозы. Ужесточение ответственности за посягательства с использованием информационно-телекоммуникационных технологий, учитывая неограниченность круга потенциальных жертв от преступных действий и размеры причиняемого ущерба, должно быть реализовано и в отечественном законодательстве. Интересными для имплементации представляются реализованные в законодательстве Франции и Литвы нормы, предусматривающие ответственность лиц, принимающих поддельную платежную карту к оплате.

Противоречива ситуация в правоохранительной среде: международное законодательство и правовые акты большинства государств законодательно указывают на возможность и необходимость использования цифровых и современных технологий, однако лишь в общем виде, – не существует правового акта, который бы в полном объеме регулировал работу органов правопорядка с цифровыми и компьютерными технологиями.

В Уголовном кодексе Франции нормы, предусматривающие ответственность за компьютерные преступления, содержатся в двух книгах. Так, в книгу вторую («О преступлениях и проступках против личности»), содержащую главу «О посягательствах на личность», включены составы таких преступлений, как незаконные действия с личными данными в телекоммуникационных системах. В книге третьей («Об имущественных преступлениях и проступках») размещена глава «О посягательствах на системы автоматизированной обработки данных», нормы которой предусматривают уголовную ответственность за ее неправомерное использование. Из этого следует, что уголовно-правовой охране подлежат личные данные, а также телекоммуникационные системы. Специальных норм о хищениях, совершаемых с использованием компьютерной информации, Уголовный кодекс Франции не содержит.

Англосаксонская правовая система не предусматривает кодификацию законодательства, в связи с чем в Великобритании ответственность за совершение компьютерных преступлений устанавливают различные статуты: Закон о неправомерном использовании компьютера, Закон о телекоммуникациях, Закон об электронном сообщении, а также Закон о защите персональных данных, Закон о телевизионных лицензиях, Закон о борьбе с обманом в области социального обеспечения. Однако ни один из перечисленных статутов напрямую не устанавливает ответственность за совершение хищений в сфере компьютерной информации. Законом о неправомерном использовании компьютера предусмотрена ответственность за несанкционированный доступ к компьютерным материалам, несанкционированный доступ с намерением совершить или облегчить совершение дальнейших правонарушений, несанкционированные действия с намерением нанести ущерб в отношении нарушения работы компьютера, несанкционированные действия, вызывающие или

создающие опасность значительного ущерба, а также за изготовление, поставку или получение изделий для использования в вышеуказанных правонарушениях. Компьютерная информация в одних случаях выступает объектом преступления, в других – предметом, средством или способом совершения преступления.

В Уголовном кодексе Германии компьютерное мошенничество выделено в отдельное преступление. Параграфом 263а установлена ответственность за действия в целях получения для себя или третьего лица противоправной имущественной выгоды, которыми наносится вред имуществу другого лица посредством воздействия на результат обработки данных компьютера путем составления неправильных программ, использования неправильных или неполных данных, несанкционированного применения данных или иного неправомочного воздействия на процесс обработки данных. Компьютерная информация в этом случае выступает способом совершения хищения.

Статьей 246.11 Уголовного кодекса Японии предусмотрена ответственность за противоправное извлечение выгоды посредством изготовления электромагнитной записи, противоречащей истине: установлено, что лицо, которое путем подачи в ЭВМ, используемую в профессиональной деятельности другого лица, сфальсифицированной информации либо неправомерной команды предоставило для использования в ведении дел другого лица противоречащую истине электромагнитную запись относительно приобретения, утраты либо изменения имущественного права и таким образом прибрело противоправную имущественную выгоду или позволило это иному лицу, – наказывается лишением свободы с принудительным физическим трудом на срок до 10 лет. Кроме того, уголовная ответственность за незаконное проникновение в компьютерные системы и информационные сети в целях кражи, порчи информации, а также использование в целях извлечения дохода и причинения ущерба законным владельцам

предусмотрена в законе «О несанкционированном проникновении в компьютерные сети».

При построении работы правоохранительных структур и подборе кадров следует обращать внимание и на международный опыт. Так, в Германии и Англии используется позитивный опыт криминальной цифровой разведки, которая в закрытом режиме работает с преступниками и террористами. Исследователи, правоведы и практики закономерно отмечают, что создание и становление подразделений киберполиции и криминальной разведки – необходимые точки роста для всей международной правоохранительной системы. Сейчас при достаточном количестве профильных специалистов их нехватка остро ощущается именно в системе МВД России. В недалеком прошлом было возможно взять людей, закончивших сторонние вузы, сразу на соответствующие их квалификации должности, например при знании иностранного языка. После соответствующей проверки подобные кадры охотно принимали даже в структуры Интерпола. Сегодня это практически невозможно: основной штат подобных организаций формируется исключительно из сотрудников правоохранительных органов. Одновременно с этим следует учитывать, что сейчас проблематично найти специалиста в начальных звеньях системы МВД России, владеющего хотя бы одним иностранным языком. В связи с этим закономерной становится проблема, когда в отделы по борьбе с компьютерными преступлениями набирают из ведомственных вузов, практически полностью пренебрегая людьми, которые получили технические или цифровые специальности.

Многие меры могут не возыметь должного результата, так как даже применение автоматизированных процессов в деятельности органов правопорядка развитых стран не обошлось без недостатков в информационной обеспеченности. В частности, сами работники отмечают следующие аспекты: недостаточная оснащенность современной компьютерной техникой (особенно

на уровне отделов полиции); недостаточная пропускная способность локальных сетей; несовершенство программного обеспечения; ненадежность оборудования, не компенсируемая одновременным требованием ведения учета в бумажной форме; отсутствие долгосрочной технической поддержки со стороны разработчиков.

Слабую готовность полиции к борьбе с киберпреступностью еще более явной сделала пандемия коронавирусной инфекции. Силы полиции были сосредоточены на других направлениях, что привело к существенному росту цифровых краж и мошенничеств. Такая проблема свойственна не только России, но и зарубежным странам: так, в Германии мошенники создали сайт министерства экономики одной из территориальных единиц страны и занимались взломом карт и кражей денежных средств, выманивая персональные данные.

Подобные ситуации случаются на фоне того, что и в России, и за рубежом проводятся постоянные совещания, коллегии и круглые столы, посвященные киберпреступности и, соответственно, кибербезопасности. Международный характер совершаемых преступных посягательств в цифровой среде подтверждается и существующей практикой. Так, в 2019 г. полицейские пресекли деятельность банды, похитившей десятки тысяч персональных данных граждан России и Евросоюза из банковских организаций. Правоохранительными органами Европейского союза и России их деятельность была совместно раскрыта.

В развивающихся странах по-прежнему существуют значительные пробелы в борьбе с киберпреступностью. Те страны, которые быстро переходят в цифровую форму, но еще не в полной мере способны обеспечить кибербезопасность, испытывают острую необходимость в использовании опыта частного сектора для наращивания потенциала в области обороны и расследований. За изощренными и громкими атаками, такими как ограбле-

ние Центрального Банка Бангладеш в 2016 г., последовали аналогичные атаки в России, а также в Центральной и Восточной Азии, Латинской Америке, Африке и на Ближнем Востоке.

Интернет-преступность затронула даже традиционные формы преступности. В прошлом преступник входил в банк, чтобы совершить ограбление, сегодня же этот преступник может ограбить банк удаленно, используя цифровые средства. Этот сдвиг сделал почти все преступления особенно сложными и глобальными по умолчанию. Ответные меры правоохранительных органов также должны носить международный характер. Такое изменение криминогенного ландшафта требует масштабируемого и воспроизводимого регионального и международного сотрудничества в рамках экосистемы безопасности между государственным и частным секторами. Следственный ландшафт, состоящий из поставщиков услуг связи, технологических компаний, компаний по разведке угроз и безопасности, наряду с правоохранительными органами может выступать мощной силой в международном сотрудничестве.

В таких условиях очередной рывок может быть сделан при использовании последних достижений науки и техники. В качестве примера можно привести технологию больших данных, которая представляет собой одновременную обработку больших объемов сведений из разных источников. При охране правопорядка к таким сведениям могут относиться GPS-сигналы от автомобилей или технических устройств, информация из банковских структур, анализ социальных сетей и сайтов. Технологию больших данных можно использовать, например, для организации безопасности транспортного и дорожного движения, предупреждения преступлений, террористических и экстремистских актов, выявления экономических преступлений. Особенно ярко необходимость в использовании подобных технологий возникает именно при переходе преступности в цифровое пространство.

Противоправные деяния совершаются не только в экономической сфере, но и во всех остальных, в частности в торговле наркотическими и психотропными веществами. Функциональные возможности больших данных «позволят правоохранительным органам в короткие сроки анализировать большие объемы различной информации, моделировать процесс принятия решений по обеспечению безопасности и прогнозировать их эффективность»[1].

Также в совокупности с другими технологиями, например глубинным обучением (Deep learning), возможен розыск лиц, скрывающихся от правоохранительных органов, путем мониторинга социальных сетей и систем видеофиксации. Например, система распознавания лиц FindFace Security, внедренная в нескольких городах в период проведения чемпионата мира по футболу в России, позволила задержать более 180 правонарушителей, часть из которых находилась в федеральном розыске. Приложение Spot App дает возможность зафиксировать нарушение Правил дорожного движения с мобильного телефона и направить сообщение об этом непосредственно в ГИБДД МВД России.

Интерес представляет мнение ряда ученых, которые помимо выделения основных проблем деятельности органов внутренних дел в условиях цифровизации предлагают создать обособленную структуру, которая будет заниматься раскрытием и расследованием цифровых преступлений: для трансформации традиционной правоохранительной деятельности в цифровую экономику необходимо полностью оцифровать правоохранительную оперативную обстановку, администрировать же цифровую оперативную обстановку должна обособленная правоохранительная организация сетевого типа[2].

---

[1] Никитин Е. В. О новых возможностях применения цифровых технологий в правоохранительной деятельности // Правоохранительная деятельность и электронное правосудие. 2018. № 4 (19). С. 57.

[2] Например: Тагиров З. И. Цифровая оперативная обстановка, цифровое имя человека и сетевая (цифровая) правоохранительная деятельность в отечественной модели цифровой экономики // Вопросы безопасности. 2018. № 4.

Обобщая сказанное ранее, можно выделить основные проблемы современной правоохранительной системы в условиях цифровизации:

1. Существующая двойственность документооборота. Так, правоохранительная информация на аналоговых или бумажных носителях не может быть интегрирована с цифровой информацией и геоинформационной основой современных технологий.

2. Оперативная идентификация подозреваемых лиц по традиционному, неуникальному имени человека, а не по цифровым личным кодам.

3. Низкий уровень использования ГЛОНАСС-устройств, GPS-координат и географических координат при составлении процессуальных документов.

4. Отсутствие идентифицирующих лично-служебных цифровых кодов у сотрудников органов правопорядка.

5. Умозрительное установление в существующей модели анализа оперативной обстановки связи методами личного сыска самими служащими правоохранительных органов без применения информационных технологий.

Процесс фиксации и подачи заявления, опросы лиц, которых подозревают в совершении преступлений или профилактируют в связи с совершением ими административных правонарушений, следует переводить в цифровой режим с последующим анализом на уровне больших данных с использованием алгоритмов искусственного интеллекта и нейросетей[1].

Говоря о проблемах в деятельности правоохранительных органов в условиях повсеместной цифровизации, следует подробнее остановиться на электронном контроле, который осуществляется в целях пресечения, предотвращения и раскрытия преступных посягательств. Вместе с тем данную тему нельзя рассматривать в отрыве от международного и зарубежного опыта.

---

[1] См.: Овчинский В. С. Технологии будущего против криминала : учебник. М. : Книжный мир. 2019.

Когда мы говорим об электронном контроле, то подразумеваем прежде всего два его вида:

1. Контроль государства над социальными сетями в целях пресечения фактов распространения детской порнографии, насильственного экстремизма, оружия, наркотиков, призывов к суициду.

2. Видеоконтроль в общественных местах. Существуют две основных модели видеоконтроля: китайская и западная. Российский видеоконтроль в основном развивается по методологии западного с некоторыми элементами китайского.

Китай идет по пути тотального видео- и цифрового контроля. До конца 2020 г. планировалась установка более 600 млн видеокамер. Вместе с тем полицейские повсеместно оснащаются специальными очками, дисплеями и иными техническими приспособлениями, которые способны выдать всю информацию о гражданах в течение нескольких секунд. Видеоконтроль является ядром более широкой государственной системы – китайской государственной системы социального кредита. Суть ее состоит в создании саморегулирующейся тотальной системы, которая с помощью манипуляторных запугивающих инструментов подводит каждого гражданина к правомерному поведению. Так, возможно, будет выглядеть общество будущего, в котором существует специальный рейтинг, позволяющий получить продвижение по службе и возможность выезда за границу, получить кредит или учиться в престижных учебных заведениях.

Европейские страны тоже развивают систему видеоконтроля, в одном только Лондоне установлено более 500 тыс. камер видеонаблюдения. В Москве, например, только планируется установка в два раза меньшего количества камер. Однако система распознавания лиц и видеоконтроля неизбежна и необходима, так как существенно снижает не только возможность совершения преступления, но и риски при расследовании и поимке преступника.

В ключе проводимого исследования интерес представляет также и цифровой подход к осуществлению правосудия, что, несомненно, тесно связано с деятельностью органов внутренних дел и иных правоохранительных органов. В ряде стран уже вплотную переходят к вопросу о возможности осуществления судебной деятельности искусственным интеллектом в условиях быстро развивающихся современных отношений. В качестве примера можно привести опыт бразильских коллег, которыми используется специальная программа «Электронный судья» – особая экспертная система, которая на основе показаний свидетелей, а также вещественных доказательств при транспортных происшествиях дает аналитическое заключение, на основе которого выносится судебное решение. «Электронный судья» способен самостоятельно квалифицировать правонарушение и теоретически обосновать возможный приговор[1]. Такая система не в полной мере является элементом электронного правосудия, но уже близко подходит к нему в привычном понимании. Гуманность и обоснованность подобного подхода правительств некоторых государств к рассмотрению правонарушений вызывают вопросы, однако позиции высших судебных инстанций в иностранных государствах и Российской Федерации позволяют говорить об осознанном применении подобных систем в правовом поле расследования и раскрытия преступлений.

В качестве еще одного примера функционирования электронного правосудия за рубежом можно привести подход Германии, где разрабатывается возможность принятия судебного решения специализированной системой по искам о детских пособиях. В Китае и США уже сегодня используется специальное программное обеспечение, которое помогает в принятии судебного решения по различным категориям дел, в том числе и уго-

[1] Brazil – Supreme Court // Brazil Court. URL: http://www.v-brazil.com/government/judiciary-branch/supreme-court.html.

ловного характера, путем систематизации составов преступлений и обобщения полученных данных, отраженных в фабуле дела. В США также применяется интересный подход к осуществлению цифрового правосудия, основанный на особенностях англосаксонской системы права, в которой используется судебный прецедент. Программа оценивает вынесенные ранее судебные решения по определенной категории дел и дает вероятностные и возможные судебные решения на основе ранее принятых. По словам создателя, это позволит обеспечить взаимодействие между человеком и машиной для взаимного компенсирования их недостатков[1].

Дальше всего в этом вопросе пошли законодатели Сингапура, где уже на протяжении длительного времени все дела по административным правонарушениям рассматриваются без участия живого судьи.

Вообще, вопрос об использовании искусственного интеллекта в судебных системах был впервые рассмотрен на уровне Европейской комиссии в апреле 2018 г. Результаты опроса свидетельствуют о том, что министерства юстиции государств – членов ЕС широко пользуются инструментами искусственного интеллекта как на федеральном, так и на местном уровне. Однако при обработке результатов опроса удалось установить, что практически во всех случаях под такими инструментами понимались либо корпоративные информационно-аналитические системы, т. е. хранилища документации, оснащенные визуализаторами и поисковиками, либо стандартные статистические пакеты, обрабатывающие стандартные цифровые данные. Ни первые, ни вторые программные комплексы не являются искусственным интеллектом, а относятся к предыдущей стадии интеллектуального софта – дата-майнингу.

---

[1] Толкователи судей: в США разработали программу, угадывающую 7 из 10 решений Верховного суда // Право.ru. URL: https://pravo.ru/review/view/124329.

Исследователи проблем использования искусственного интеллекта в правосудии и правоохранительной деятельности нередко задаются вопросами этичности и правомерности. Высказываются предположения о том, что использование искусственного интеллекта таит опасность сделать человека, его права и свободы уязвимыми, а само правосудие – бесчеловечным и формальным.

Чтобы развеять эти сомнения, в мировом сообществе делаются первые шаги. Так, в декабре 2018 г. Европейской комиссией одобрена Европейская этическая хартия использования искусственного интеллекта в судебной и правоохранительной системах. В феврале следующего года Центр европейских политических исследований при Евросоюзе опубликовал доклад об этических, правовых и политических принципах регулирования развития и применения искусственного интеллекта относительно любых направлений деятельности. В США Партнерство по искусственному интеллекту, в которое входит более 80 корпоративных разработчиков и пользователей, в начале 2019 г. опубликовало отчет об алгоритмических инструментах оценки рисков в системе уголовного правосудия США. 25 мая 2019 г. Организация экономического развития и сотрудничества поддержала принципы ответственного управления надежным искусственным интеллектом.

Говоря о проблемах деятельности органов внутренних дел в условиях цифровизации, необходимо иметь в виду и оперативный контроль, который сегодня осуществляется с помощью технологий четвертой промышленной революции. Так, здесь накоплен огромный опыт подразделений ФБР, британской полиции, группы ePOOLICE, созданной при Европейском союзе. В основе их деятельности лежит работа с большими данными (структурированными и неструктурированными), открытыми и закрытыми разведывательными (оперативно-разыскными) данными, материалами уголовных дел, данными аудио- и видеонаблюдения.

Применяемые системы работают по принципу выявления ранних признаков организованной преступной деятельности через выявление подозрительных транзакций по отмыванию денег, полученных в результате преступной деятельности.

В Руководстве для дискуссий XIV конгресса ООН «О предупреждении преступности» вопросу цифровизации правоохранительной системы и модернизации методов борьбы с преступностью уделено основное внимание. В целях усиления контроля за преступными посягательствами необходимо срочно разработать действенные механизмы контроля криптовалют для предотвращения отмывания денежных средств. Существенное внимание следует уделить разработке средств и методов борьбы с организованной преступностью в виртуальной среде, пресечению распространения оружия, наркотических и психотропных веществ.

При осуществлении контроля над преступностью сегодня следует осознавать, что масштаб и сложность возникающих проблем нарастают подобно снежному кому. Преступность во многом связана с региональными вооруженными противостояниями в результате давних экономических, политических, конфессиональных конфликтов, мировыми и национальными демографическими кризисами, спонтанным развитием технологий, создающих угрозу существованию человечества. Преступность можно контролировать только в комплексе с вопросами смягчения негативных последствий перечисленных глобальных проблем.

ЗАКЛЮЧЕНИЕ

Сегодня практически никто не ставит под сомнение тот факт, что в ближайшем будущем компьютеризация различных сфер общественных отношений лишь увеличится. Это, в свою очередь, не только приведет к положительным последствиям, но и породит комплекс социальных проблем и криминальных угроз.

Вместе с тем очевидно: какими бы ни были негативные последствия информатизации, никто и никогда не откажется от интернет-банкинга, высокотехнологичной медицины, социальных сетей, многопользовательских онлайн-игр и т. д.

Количество зарегистрированных преступлений в сфере информационных технологий за последние три года увеличилось более чем на 300 %, при этом раскрываемость подобных преступлений крайне низка – чуть более 20 %. Преступления и иные правонарушения в сфере информационных технологий являются наиболее латентными из всех правонарушений, поскольку лица, сталкивающиеся с получением фишинговых писем, взломом своих страниц в социальных сетях, попыткой хищения электронных денежных средств или средств с банковского счета, не всегда обращаются с заявлением в правоохранительные органы.

Современное общество столкнулось с необходимостью решения двух задач: 1) построения эффективной системы защиты информации и информационной инфраструктуры; 2) глубокой модернизации положений законодательства в соответствии с реалиями глобальной информатизации большинства сфер общественной жизни, необходимости эффективно противодействовать киберпреступности.

Несмотря на масштаб и сложность проблемы эффективного противодействия преступлениям и административным правонарушениям, совершаемым с использованием информационных технологий, предполагается, что модернизация законодательства должна осуществляться крайне осторожно, по принципу минимизации вносимых поправок. Нет никакой необходимости

сплошного насыщения административно-правовых и уголовно-правовых норм указанием на возможность совершения правонарушений в сфере информационных технологий, – такие оговорки должны иметь место только при очевидном несоответствии законодательства современным угрозам.

Взаимосвязь современных программно-аппаратных комплексов, технических навыков и знаний в области права позволит успешно противодействовать новым вызовам и угрозам правонарушителей.

Неотложной и значимой задачей выступает формирование единообразной правоприменительной практики в условиях имеющегося нормативного материала, что, как представляется, потребует не только определенного времени, но и научных разработок, способствующих противодействию новым вызовам противоправной деятельности в сфере киберпреступлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Основная литература

1. Актуальные проблемы уголовного права : курс лекций / под ред. О. С. Капинус. – М. : Академия Генеральной прокуратуры Российской Федерации, 2015. – 484 с.

2. Арзамасцев, М. В. К вопросу об уголовно-правовой классификации киберпреступлений / М. В. Арзамасцев // Актуальные вопросы права и отраслевых наук. – 2017. – № 1 (3). – С. 11–17.

3. Афанасьев, В. Г. Социальная информация и управление обществом / В. Г. Афанасьев. – М. : Политиздат, 1975. – 408 с.

4. Быков, В. М. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы : монография / В. М. Быков, В. Н. Черкасов. – М. : Юрлитинформ, 2015. – 325 с.

5. Вахрушев, Д. С. Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления / Д. С. Вахрушев, О. В. Железов // Вестник евразийской науки. – 2014. – № 5 (24). – URL: https://cyberleninka.ru/article/n/kriptovalyuta-kak-fenomen-sovremennoy-informatsionnoy-ekonomiki-problemy-teoreticheskogo-osmysleniya (дата обращения: 09.12.2019).

6. Венгеров, А. Б. Право и информация в условиях автоматизации управления. Теоретические проблемы : автореф. дис. … д-ра юрид. наук : 12.00.01 / А. Б. Венгеров. – М., 1975. – 25 с.

7. Володченко, В. С. Современные информационные технологии и их виды / В. С. Володченко, Д. С. Ланцова, О. Ю. Ивлев // Достижения науки и образования. – 2018. – № 18 (40). – URL: https://cyberleninka.ru/article/n/sovremennye-informatsionnye-tehnologii-i-ih-vidy-1 (дата обращения: 10.04.2020).

8. Воронкова, Д. К. Комплексная судебная компьютерно-техническая и видеотехничская экспертиза / Д. К. Воронкова,

А. С. Воронков, А. М. Пилипчак // Modern Science. – 2019. – № 12-1. – С. 300–306.

9. Галиакбаров, Р. Р. Нетрадиционные аспекты множественности в уголовном праве / Р. Р. Галиакбаров // Уголовно-правовые средства борьбы с преступностью: межвузовский сборник научных трудов. Омск : Омская высшая школа милиции МВД СССР, 1983. – С. 19–25.

10. Гилинский, Я. И. Криминологические основы уголовного права в эпоху постмодерна / Я. И. Гилинский // Криминологические основы уголовного права: материалы X Российского конгресса уголовного права, состоявшегося 26–27 мая 2016 г. / [отв. ред. В. С. Комиссаров]. – М. : Юрлитинформ, 2016. – С. 294–298.

11. Гончар, В. В. О важности формирования единообразного понятийного аппарата, необходимого для расследования преступлений в сфере компьютерной информации / В. В. Гончар // Вестник экономической безопасности. – 2018. – № 1. – С. 225–230.

12. Гончаренко, Л. П. Цифровизация национальной экономики / Л. П. Гончаренко, С. А. Сыбачин // Вестник ГУУ. – 2019. – № 8. – URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-natsionalnoi-ekonomiki (дата обращения: 03.04.2020).

13. Гринберг, М. С. Научно-технический прогресс и технические преступления / М. С. Гринберг // Вестник ОмГУ. – 2010. – № 1. – URL: https://cyberleninka.ru/article/n/nauchno-tehnicheskiy-progress-i-tehnicheskie-prestupleniya (дата обращения: 12.04.2020).

14. Гришаев, П. И. Соучастие по советскому уголовному праву / П. И. Гришаев, Г. А. Кригер. – М. : Госюриздат, 1959. – 255 с.

15. Гузеева, О. С. Преступления, совершаемые в российском сегменте сети Интернет : монография / О. С. Гузеева. – М. : Академия Генеральной прокуратуры Российской Федерации, 2015. – 136 с.

16. Дворецкий, М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания : монография / М. Ю. Дворецкий. – Тамбов : Издательство Тамбовского государственного университета, 2003. – 197 с.

17. Дж. Хосп. О криптовалюте просто: Биткоин, эфириум, блокчейн, децентрализация, майнинг, ICO & Co / Дж. Хосп. – СПб. : Питер, 2019. – 256 с. – (IT для бизнеса).

18. Евтеева, Е. В. Информационно-техническое обеспечение информационных технологий / Е. В. Евтеева // Вестник ВУиТ. – 2015. – № 2 (24). – URL: https://cyberleninka.ru/article/n/informatsionno-tehnicheskoe-obespechenie-informatsionnyh-tehnologiy (дата обращения: 09.04.2020).

19. Ефремова, М. А. Уголовно-правовая охрана информационной безопасности : дис. … д-ра юрид. наук : 12.00.08 / М. А. Ефремова. – М., 2018. – 427 с.

20. Зорькин, В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума / В. Д. Зорькин // Российская газета. – URL: https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html (дата обращения: 23.05.2020).

21. Зуйков, Г. Г. Поиск преступников по признакам способов совершения преступлений : учебное пособие / Г. Г. Зуйков. – М. : Высшая школа МВД СССР, 1970. – 189 с.

22. Калиниченко, И. А. О приоритетных направлениях подготовки кадров для органов внутренних дел Российской Федерации в условиях информатизации общества / И. А. Калиниченко // Вестник Московского университета МВД России. – 2020. – № 3. – С. 11–14.

23. Карпова, Д. Н. Социотехнический поворот в исследовании цифровизации общества / Д. Н. Карпова, А. С. Проскурина // Власть. – 2020. – № 1. – URL: https://cyberleninka.ru/article/n/sotsiotehnicheskiy-povorot-v-issledovanii-tsifrovizatsii-obschestva (дата обращения: 12.04.2020).

24. Кауфман, М. А. Некоторые вопросы применения Общей части УК РФ / М. А. Кауфман // Государство и право. – 2000. – № 6. – С. 56–60.

25. Козаев, Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства) : монография / Н. Ш. Козаев ; под ред. А. В. Наумова. – М. : Юрлитинформ, 2015. – 218 с. – (Уголовное право).

26. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. … канд. юрид. наук : 12.00.12 / В. В. Коломинов. – Иркутск, 2017. – 211 с.

27. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / под ред. С. В. Дьякова, Н. Г. Кадникова. – 5-е изд., перераб. и доп. – М. : Юриспруденция, 2017. – 1072 с.

28. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / [В. П. Верин и др.] ; отв. ред. В. И. Радченко ; науч. ред. А. С. Михлин. – М. : Проспект, 2008. – 699 с.

29. Кригер, Г. А. Ответственность за хищение государственного или общественного имущества по советскому уголовному праву / Г. А. Кригер. – М. : Издательство Московского университета, 1957. – 208 с.

30. Крылов, В. В. Основы криминалистической теории расследования преступлений в сфере информации : дис. … д-ра юрид. наук : 12.00.09 / В. В. Крылов. – М., 1998. – 334 с.

31. Лопашенко, Н. А. Уголовно-правовая и криминологическая политика государства в области высоких технологий / Н. А. Лопашенко // Информационные технологии и безопасность : сборник научных трудов Международной конференции. – Киев, 2003. – С. 89–97.

32. Мазуров, М. Е. Моделирование научно-технического прогресса / М. Е. Матузов // Статистика и экономика. – 2015. – № 5. – С. 108–110.

33. Малахов, И. П. Соучастие и групповая организованная преступность / И. П. Малахов // Правоведение. – 1994. – № 5–6. – С. 125–126.

34. Малыковцев, М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ : дис. … канд. юрид. наук : 12.00.08 / М. М. Малыковцев. – М., 2006. – 186 с.

35. Маслакова, Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. … канд. юрид. наук : 12.00.08 / Е. А. Маслакова. – М., 2008. – 198 с.

36. Матейкович, М. С. Об уголовной ответственности за преступления в сфере незаконного оборота наркотиков, совершенные организованными группами и преступными сообществами М. С. Матейкович // Российская юстиция. – 2015. – № 12. – С. 25–27.

37. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». – 2013. – Режим доступа: по расписанию.

38. Молчанова, Т. В. Факторы, обуславливающие мошенничество, совершенное с использованием информационно-телекоммуникационных технологий / Т. В. Молчанова, В. А. Аксенов // Вестник экономической безопасности. – 2020. – № 2. – С. 93–98.

39. Мороз, Н. О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий / Н. О. Мороз // Вестник Полоцкого государственного университета. Серия D: Экономические и юридические науки. – 2011. – № 14. – С. 147–148.

40. Никитин, Е. В. О новых возможностях применения цифровых технологий в правоохранительной деятельности / Е. В. Никитин // Правоохранительная деятельность и электронное правосудие. – 2018. – № 4 (19). – С. 55–59.

41. Овчинский, В. С. Технологии будущего против криминала : учебник / В. С. Овчинский. – М. : Книжный мир, 2019. – 288 с.

42. Осипенко, А. Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления / А. Л. Осипенко // Вестник Воронежского института МВД России. – 2016. – № 3. – С. 83–90.

43. Основы сетевых технологий : учебник для вузов / Н. А. Руденков, Л. И. Долинер. – Екатеринбург : Издательство Уральского федерального университета, 2011. – 300 с.

44. Падалко, А. Цифровые активы: новый объект гражданского права и вопросы его налогообложения при первом приближении / А. Падалко // Rodl & Partner. – URL: https://www.roedl.net/ru/ru/home.html (дата обращения: 23.05.2019).

45. Пикуров, Н. И. Квалификация преступлений с бланкетными признаками состава : монография / Н. И. Пикуров. – М. : Российская академия правосудия, 2009. – 288 с.

46. Преступления в сфере компьютерной информации: квалификация и доказывание : учебное пособие / под ред. Ю. В. Гаврилина. – М. : Юридический институт МВД России, 2003. – 245 с.

47. Пропастин, С. В. Оценка следователем результатов компьютерной экспертизы / С. В. Пропастин // Уголовный процесс. – URL: https://www.ugpr.ru/article/199-otsenka-sledovatelem-rezultatov-kompyuternoy-ekspertizy (дата обращения: 14.05.2020).

48. Пудовочкин, Ю. Е. Квалификация соучастия в преступлении. Судебная практика : научно-практическое пособие / Ю. Е. Пудовочкин. – М. : Российский государственный университет правосудия, 2017. – 174 с. – (Библиотека российского судьи).

49. Рарог, А. И. Проблемы квалификации преступлений по субъективным признакам : монография / А. И. Рарог. – М. : Проспект, 2015. – 229 с.

50. Расследование неправомерного доступа к компьютерной информации : учебное пособие / под ред. Н. Г. Шурухнова. – М. : Московский университет МВД России, 2004. – 256 с.

51. Рекомендации по изъятию компьютерной техники и носителей информации при проведении обыска. Варианты описания объектов, содержащих компьютерную информацию : методические рекомендации. – Брянск : ЭКЦ УМВД России по Брянской области, 2013.

52. Решетников, А. Ю. Конструкция состава преступления и ее влияние на установление момента его окончания / А. Ю. Решетников, Л. А. Букалерова // Уголовное наказание в России и за рубежом: проблемы назначения и исполнения (к 10-летию принятия Европейский пенитенциарных правил): сборник материалов Международной научно-практической конференции : в 2 ч. / под общ. ред. П. В. Голодова. – Вологда : Вологодский институт права и экономики ФСИН России, 2017. – С. 249–251.

53. Решетников, А. Ю. Квалификация деяния исполнителя при добровольном отказе от доведения преступления до конца / А. Ю. Решетников // Законность. – 2017. – № 8. – С. 41–45.

54. Решетников, А. Ю. Квалификация неоконченных преступлений при наличии признаков совокупности преступлений / А. Ю. Решетников // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2016. – № 4 (54). – С. 81–88.

55. Рожкова, М. А. Права на доменное имя // Право в сфере Интернета : сборник статей / рук. авт. кол. и отв. ред. М. А. Рожкова. – М. : Статут, 2018. – С. 195–223. – URL: https://cctld.ru/files/books/rozhkova_asp.pdf (дата обращения: 01.04.2020).

56. Рожкова, М. А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым / М. А. Рожкова // Закон.ру. – URL: https://zakon.ru/blog/2018/6/13/cifrovye_aktivy_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe_s_cifrovym (дата обращения: 01.04.2020).

57. Ролик, А. И. Преступление, предусмотренное ст. 2281 УК РФ: спорные вопросы характеристики / А. И. Ролик // Lex Russia. – 2014. – № 9. – С. 1079–1092.

58. Романова, А. С. Борьба с преступностью в компьютерных сетях «глубинного» интернета / А. С. Романова // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы Всероссийской научно-практической конференции. – Иркутск : Восточно-Сибирский институт МВД России, 2016. – С. 122–127.

59. Российское уголовное право : учебник : в 2 т. / [Г. Н. Борзенков и др.] ; под ред. Л. В. Иногамовой-Хегай, В. С. Комиссарова, А. И. Рарога. – 3-е изд. – М. : Проспект, 2010.

60. Россинская, Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е. Р. Россинская // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2019. – № 5. – С. 31–44.

61. Россинская, Е. Р. Судебная компьютерно-техническая экспертиза / Е. Р. Россинская, А. И. Усов. – М. : Право и закон, 2001. – 416 с. – (Практическая юриспруденция. Судебная экспертиза).

62. Россинская, Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е. Р. Россинская. − М. : Норма, 2006. – 656 с.

63. Русскевич, Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учебное пособие / Е. А. Русскевич. – М. : Инфра-М, 2017. – 116 с. – (Высшее образование. Магистратура).

64. Сабиров, Р. Д. Содержание признака насилия в групповых посягательствах на собственность / Р. Д. Сабиров // Проблемы совершенствования законодательства по укреплению

правопорядка и усиление борьбы с правонарушениями: Межвузовский сборник научных трудов. – Свердловск : Свердловский юридический институт, 1982. – С. 117–125.

65. Смолина, А. Р. Методологическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы : дис. … канд. техн. наук : 05.13.19. – Томск, 2017. – 132 с.

66. Совокупность преступлений: проблемы теории и практики квалификации : монография / [А. Е. Пудовочкин и др.]. – М. : Российский государственный университет правосудия, 2016. – 364 с. – (Библиотека российского судьи).

67. Степанов, А. Н. Информатика для студентов гуманитарных специальностей : учебное пособие для студентов вузов, обучающихся по гуманитарным и социально-экономическим направлениям и специальностям / А. Н. Степанов. – 3-е изд. – СПб. : Питер, 2002. – 604 с. – (Учебник для вузов).

68. Судебная экспертиза: типичные ошибки / под ред. Е. Р. Россинской. – М. : Проспект, 2019. – 642 с.

69. Тагиров, З. И. Цифровая оперативная обстановка, цифровое имя человека и сетевая (цифровая) правоохранительная деятельность в отечественной модели цифровой экономики / З. И. Тагиров // Вопросы безопасности. – 2018. – № 4. – С. 28–51.

70. Тер-Акопов, А. А. Преступление и проблемы нефизической причинности в уголовном праве : монография / А. А. Тер-Акопов. – М. : Юркнига, 2003. – 480 с.

71. Типовая методика исследования информации в мобильных телефонах / [О. В. Тушканова и др.]. – М. : ЭКЦ МВД России, 2013.

72. Типовая методика исследования информации, содержащейся в мобильных телефонах / [О. В. Тушканова и др.]. – М. : ЭКЦ МВД России, 2014.

73. Типовые экспертные методики исследования вещественных доказательств : Ч. I / под ред. Ю. М. Дильдина ; общ. ред. В. В. Мартынова. – М. : ЭКЦ МВД России, 2010. – 568 с.

74. Уголовное право: Особенная часть : учебник / под ред. А. И. Рарога. – М. : Проспект, 2009. – 600 с.

75. Федорович, В. Ю. Что такое «киберпреступление»? / В. Ю. Федорович // Вестник Московского университета МВД России. – 2020. – № 3. – С. 15–17.

76. Фролов, А. А. Исследование механизмов рассмотрения запрещенного содержимого в Darknet / А. А. Фролов, Д. С. Сильнов // Современные информационные технологии и ИТ-образование. – 2017. – № 4. – С. 216–224.

77. Хабриева, Т. Я. Право в условиях цифровой реальности / Т. Я. Хабриева, Н. Н. Черногор // Журнал российского права. – 2018. – № 1 (253). – URL: https://cyberleninka.ru/article/n/pravo-v-usloviyah-tsifrovoy-realnosti (дата обращения: 14.03.2020).

78. Хилюта, В. В. Вопросы квалификации преступлений против собственности, не являющихся хищением : научно-практическое пособие / В. В. Хилюта. – Минск : Пересвет, 2013. – 150 с.

79. Химичева, О. В. Цифровизация как тренд развития современного уголовного процесса / О. В. Химичева, А. В. Андреев // Вестник Московского университета МВД России. – 2020. – № 3. – С. 21–23.

80. Чупрова, А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий / А. Ю. Чупрова // Уголовное право. – 2015. – № 5. – С. 131–134.

81. Шаевич, А. А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений : монография / А. А. Шаевич. – Иркутск : Восточно-Сибирский институт МВД России, 2011. – 108 с.

82. Шестакова, И. Г. Новая темпоральность цифровой цивилизации: будущее уже наступило / И. Г. Шестакова // Научно-технические ведомости СПбГПУ. Гуманитарные и общественные науки. – 2019. – № 2. – С. 20–29.

83. Шумов, В. В. Модель безопасности государства / В. В. Шумов // УБС. – 2015. – № 58. – URL: https://cyberleninka.ru/article/n/model-bezopasnosti-gosudarstva (дата обращения: 12.04.2020).

84. Энгельгардт, А. А. Оценка преступлений как продолжаемого деяния или множественности (на примере преступлений в сфере компьютерной информации) / А. А. Энгельгардт // Право и политика. – 2014. – № 12. – С. 1860–1864.

85. Юрасов, М. Защита прав инвесторов при проведении ICO блокчейн-проектов / М. Юрасов // Закон.ру. – URL: https://zakon.ru/blog/2017/11/5/zaschita_prav_investorov_pri_provedenii_ico_blokchejn-proektov (дата обращения: 23.04.2020).

86. Ягудин, А. Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей : автореф. … дис. канд. юрид. наук : 12.00.08 / А. Н. Ягудин. – М., 2013. – 27 с.

87. Smith, J. Tor: A Dark Net Journey on How to Be Anonymous Online / J. Smith. – North Charleston : CreateSpace Independent Publishing Platform, 2017. – 50 p.

Нормативные правовые акты

1. Директива Европейского союза 2018/843 от 30 мая 2018 г., вносящая изменения в Директиву Европейского союза 2015/849 по предотвращению использования финансовой системы для целей легализации доходов, полученных преступным путем, финансирования терроризма и вносящая изменения в Директивы 2009/138/ЕК и 2013/36/ЕС // EUR-Lex. – URL: https://eur-lex.europa.eu/eli/dir/2018/843/oj (дата обращения: 16.12.2019).

2. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Собрание законодательства Российской Федерации. – 2009. – № 13. – Ст. 1460.

3. Уголовный кодекс Российской Федерации : УК : Федеральный закон № 63-ФЗ : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699 (дата обращения: 10.05.2021).

4. Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_5842 (дата обращения: 10.05.2021).

5. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 10.05.2021).

6. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_201078 (дата обращения: 10.05.2021).

7. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_220885 (дата обращения: 10.05.2021).

8. Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_296451 (дата обращения: 10.05.2021).

9. Федеральный закон от 19 июля 2018 г. № 217-ФЗ «О внесении изменений в статью 256 части первой и часть третью

Гражданского кодекса Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_302862 (дата обращения: 10.05.2021).

10. Постановление Правительства Российской Федерации от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи» // Собрание законодательства Российской Федерации. – 2007. – № 38. – Ст. 4552.

11. Постановление Правительства Российской Федерации от 30 сентября 2004 г. № 506 «Об утверждении Положения о Федеральной налоговой службе» // Российская газета. – 2004. – № 219.

12. Постановление Правительства Российской Федерации от 1 июня 2009 г. № 457 «О Федеральной службе государственной регистрации, кадастра и картографии» // Собрание законодательства Российской Федерации. – 2009. – № 25. – Ст. 3052.

13. Постановление Правительства Российской Федерации от 10 июля 2013 г. № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети „Интернет” и обновления информации об образовательной организации» // Собрание законодательства Российской Федерации. – 2013. – № 29. – Ст. 3964.

14. Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации „Информационное общество”» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_162184 (дата обращения: 10.05.2021).

15. Постановление Правительства Российской Федерации от 23 декабря 2004 г. № 835 «Об утверждении Положения о Государственной инспекции по маломерным судам Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий» // Собрание законодательства Российской Федерации. – 2004. – № 52 (ч. II). – Ст. 5499.

16. Постановление Пленума Верховного Суда Российской Федерации от 18 октября 2012 г. № 21 «О применении судами законодательства об ответственности за нарушения в области охраны окружающей среды и природопользования» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_136950 (дата обращения: 10.05.2021).

17. Постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_108437 (дата обращения: 10.05.2021).

18. Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_40412 (дата обращения: 10.05.2021).

19. Постановление Пленума Верховного Суда Российской Федерации от 30 июня 2015 г. № 30 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 года № 14 „О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами”» // Российская газета. – 2015. – № 150.

20. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_283918 (дата обращения: 10.05.2021).

21. Инструкция по организации информационного обеспечения сотрудничества по линии Интерпола : утверждена приказом МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971

от 6 октября 2006 г. (ред. от 22.09.2009) // СПС «КонсультантПлюс». – Режим доступа: по расписанию.

22. Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (вместе с Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации) (ред. от 27.06.2019) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_55315 (дата обращения: 10.05.2021).

23. Приказ МВД России от 3 декабря 2007 г. № 1144 «О системе информационного обеспечения подразделений Госавтоинспекции» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_80265 (дата обращения: 10.05.2021).

24. ГОСТ 34.003–90. Автоматизированные системы. Термины и определения : межгосударственный стандарт : издание официальное : утвержден и введен в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27 декабря 1990 г. № 3399 : дата введения 1992-01-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200006979 (дата обращения: 19.03.2020).

25. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст : дата введения 2008-02-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 19.03.2020).

26. ГОСТ Р 57429–2017. Судебная компьютерно-техническая экспертиза. Термины и определения : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2017 г. № 198-ст : введен впервые : дата введения 2017-09-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200144960 (дата обращения: 14.05.2020).

Материалы правоприменительной практики

1. Обзор судебной практики Верховного Суда Российской Федерации – 2017. – № 3 // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/cons_doc_LAW_219925 (дата обращения: 10.05.2020).

2. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 21 января 2014 г. № 72-АПУ13-63 // Бюллетень Верховного Суда Российской Федерации. – 2014. – № 8.

3. Постановление Президиума Верховного Суда Российской Федерации № 323-П08ПР / Обзор законодательства и судебной практики Верховного Суда Российской Федерации за четвертый квартал 2008 года // СПС «КонсультантПлюс». – Режим доступа: по расписанию.

4. Постановление Президиума Верховного Суда Российской Федерации № 436п96 по делу Ткаченко В. П. и Хоперского В. В. // Бюллетень Верховного Суда Российской Федерации. – 1997. – № 4.

5. Постановление Президиума Верховного Суда Российской Федерации № 495п03 по делу Бычкало и других // Бюллетень Верховного Суда Российской Федерации. – 2004. – № 3.

6. Апелляционное определение Верховного Суда Российской Федерации от 23 сентября 2015 г. по делу № 5-АПУ15-76.

7. Апелляционное определение Верховного Суда Российской Федерации от 4 апреля 2017 г. по делу № 35-АПУ17-3.

8. Постановление Президиума Высшего Арбитражного суда Российской Федерации от 16 января 2001 г. № 1192/00 по делу № А40-25314/99-15-271.

9. Апелляционное постановление Верховного Суда Республики Татарстан от 13 декабря 2016 г. по делу № 22-8753 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

10. Апелляционный приговор Судебной коллегии по уголовным делам Верховного суда Чувашской Республики от 3 июня 2015 г. по делу № 22-1054/2015 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

11. Постановление Арбитражного суда Центрального округа кассационной инстанции по проверке законности и обоснованности судебных актов арбитражных судов, вступивших в законную силу от 22 января 2020 г. по делу № А83-17242/2017 // СПС «КонсультантПлюс». – Режим доступа: по расписанию.

12. Постановление о прекращении уголовного дела Лефортовского районного суда г. Москвы от 13 января 2015 г. по делу № 1-401/2014 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

13. Постановление Октябрьского районного суда г. Иркутска от 4 сентября 2015 г. по делу № 1-461/2015 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

14. Приговор Андроповского районного суда Ставропольского края от 6 апреля 2017 г. по делу № 1-31/2017 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

15. Приговор Белгородского районного суда Белгородской области от 16 сентября 2010 г. по делу № 1-43/2010 // Судебные

и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

16. Приговор Катайского районного суда Курганской области от 18 апреля 2013 г. по делу № 1-20/2013 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

17. Приговор Московского районного суда г. Чебоксары Чувашской Республики по делу № 1-52-2012 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

18. Приговор Октябрьского районного суда г. Архангельска от 14 декабря 2015 г. по делу № 1-352/2015 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

19. Приговор Пролетарского районного суда г. Твери от 2 декабря 2014 г. по делу № 1-281/2014 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

20. Приговор Октябрьского районного суда г. Саратова от 23 января 2014 г. по делу № 1-27/2014 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

21. Приговор Октябрьского районного суда г. Ижевска от 23 июня 2014 г. по делу № 1-186/14 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

22. Приговор Советского районного суда г. Тамбова от 25 апреля 2016 г. по делу № 1-106/2016 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

23. Приговор Ленинского районного суда г. Костромы от 10 июня 2016 г. по делу № 1-77/2016 // Судебные и нормативные

акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

24. Приговор Первомайского районного суда г. Владивостока от 25 сентября 2019 г. по делу № 1-376/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

25. Приговор Московского районного суда г. Твери от 21 ноября 2016 г. по делу № 1-308/2016 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

26. Постановление Лефортовского районного суда г. Москвы от 13 января 2015 г. по делу № 1-401/2014 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

27. Приговор Канавинского районного суда г. Нижний Новгород от 29 января 2018 г. по делу 1-70/2018 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

28. Приговор Канавинского районного суда г. Нижний Новгород от 11 апреля 2018 г. по делу № 1-213/2018 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

29. Приговор Ленинского районного суда г. Махачкалы от 7 сентября 2015 г. по делу № 1-357/2015 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

30. Приговор Александровского городского суда Владимирской области от 19 августа 2015 г. по делу № 1-82/2015 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

31. Приговор Кировградского городского суда Свердловской области от 5 августа 2016 г. по делу № 1-105/2016 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

32. Приговор Ноябрьского городского суда Ямало-Ненецкого автономного округа от 11 апреля 2012 г. по делу № 1-133/2012 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

33. Приговор Бийского городского суда от 26 марта 2015 г. по делу № 1-250/2015 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

34. Приговор Северского городского суда Томской области от 4 августа 2015 г. по делу № 1-257/2015 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru (дата обращения: 10.05.2020).

35. Приговор по уголовному делу № 1-18/2018 (1-528/2017) // ГАС «Правосудие». – URL: https://bsr.sudrf.ru (дата обращения: 10.05.2020).

36. Приговор № 1-118/2019 от 6 сентября 2019 г. по уголовному делу № 1-118/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru/regular/doc/b9VnQX8BBENC (дата обращения: 15.09.2020).

37. Приговор № 1-115/2019 от 20 сентября 2019 г. по уголовному делу № 1-87/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru/regular/doc/eCrzfkGLkMl6 (дата обращения: 15.05.2020).

38. Приговор по уголовному делу № 1-5/2019 // ГАС «Правосудие». – URL: https://bsr.sudrf.ru (дата обращения: 10.05.2020).

39. Решение № 2-3192/2019 2-3192/2019~М-2853/2019 М-2853/2019 от 27 августа 2019 г. по гражданскому делу № 2-3192/2019 // Судебные и нормативные акты РФ. Суды общей юрисдикции. – URL: http://sudact.ru/regular/doc/boeC5NN2AR1S (дата обращения: 10.05.2020).

Статистические сведения

1. Всестороннее исследование проблемы киберпреступности (Вена, 25–28 февраля 2013 г.) // Управление ООН по наркотикам и преступности. – URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения: 11.07.2020).

2. Информационно-аналитические материалы Следственного департамента МВД России за 2015–2019 гг. // Официальный сайт МВД России. – URL: https://мвд.рф (дата обращения: 11.07.2020).

3. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // НПП «Гарант-сервис». – URL: https://www.garant.ru/products/ipo/prime/doc/70542118 (дата обращения: 10.05.2020).

4. Отчет Судебного департамента при Верховном Суде Российской Федерации «О числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации» за 2013 – I полугодие 2017 г.

5. Памятка следователю о проведении проверки и расследовании уголовных дел по фактам мошенничеств с использованием мобильных средств связи: подготовлена контрольно-методическим управлением Следственного департамента МВД России с использованием материалов ГСУ ГУ МВД России по Кемеровской области, СУ УМВД России по Белгородской области и ГУУР МВД России в 2015 г.

6. Состояние преступности в Российской Федерации за январь – декабрь 2019 г. // Официальный сайт МВД России. – URL: https://мвд.рф/reports/item/19412450 (дата обращения: 10.05.2020).

7. Статистические сведения Центра статистической информации ГИАЦ МВД России. – Режим доступа: форма «2-ЕГС» (492) за январь – декабрь 2019 г. Раздел: 1. Код: 1200.

8. Цифровая грамотность россиян: исследование, 2020 г. // НАФИ. – URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020 (дата обращения: 23.04.2021).

Электронные ресурсы

1. В каких странах биткоин признан официальной валютой? // Howtobuycoin. – URL: https://howtobuycoin.com/bitcoin/bitcoin-official-cryptocurrency (дата обращения: 14.03.2019).

2. В Москве суд завершил банкротство, в котором биткоины признали имуществом // РИА Новости. – URL: https://ria.ru/20180808/1526151217.html (дата обращения: 14.03.2019).

3. Дело о фишинге: как ловили хакеров-близнецов из Санкт-Петербурга // РИА Новости. – URL: https://ria.ru/incidents/20121221/915789715.html (дата обращения: 10.01.2020).

4. За четыре года на цифровую трансформацию потратят более $ 7,4 трлн // BSC. – URL: https://bsc-consulting.ru/blog/analytics/291019 (дата обращения: 23.04.2021).

5. Задержаны хакеры, взламывавшие по заказам страницы в соцсетях, почтовые ящики и занимавшиеся «прослушкой» // Официальный сайт МВД России. – URL: https://мвд.рф/news/show_102385 (дата обращения: 26.08.2019).

6. Киберпреступность вычли из ВВП // Коммерсантъ. – URL: https://www.kommersant.ru/doc/2962974 (дата обращения: 25.02.2020).

7. Компиляция // Информационный портал «Языки программирования». – URL: http://programming-lang.com (дата обращения: 10.05.2020).

8. Компьютерно-техническая экспертиза // РФЦСЭ при Минюсте России. – URL: http://www.sudexpert.ru/possib/comp.php (дата обращения: 14.05.2020).

9. Краткая история компьютерных вирусов, и что сулит нам будущее // Лаборатория Касперского. – URL: https://www.kaspersky.ru/resource-center/threats/a-brief-history-of-

computer-viruses-and-what-the-future-holds (дата обращения: 08.06.2019).

10. Ложная тревога // Российская газета. – URL: https://rg.ru/2017/09/12/reg-pfo/v-krupnyh-gorodah-rossii-evakuirovali-desiatki-shkol-vokzalov-i-tc.html (дата обращения: 15.04.2019).

11. Осужден томский хакер, взломавший сайт Президента Российской Федерации // РИА Новости. – URL: https://ria.ru/20131223/985798684.html (дата обращения: 23.04.2021).

12. Регистрация в Сбербанк Онлайн // Сбербанк. – URL: https://online.sberbank.ru/CSAFront/async/page/registration.do (дата обращения: 09.04.2020).

13. Реестр запрещенных сайтов. – URL: https://antizapret.info (дата обращения: 10.01.2020).

14. Российская «Гидра» стала крупнейшей в мире торговой площадкой по продаже наркотиков в даркнете // Новая газета. – URL: https://novayagazeta.ru/news/2019/07/25/153666-proekt-rossiyskaya-gidra-stala-krupneyshey-v-mire-torgovoy-ploschadkoy-po-prodazhe-narkotikov-v-darknete (дата обращения: 23.04.2020).

15. Телефонные террористы дозвонились в Москву // Коммерсантъ. – URL: https://www.kommersant.ru/doc/3409928 (дата обращения: 15.05.2020).

16. Толкователи судей: в США разработали программу, угадывающую 7 из 10 решений Верховного суда // Право.ru. – URL: https://pravo.ru/review/view/124329 (дата обращения: 20.04.2020).

17. Толковый словарь Дмитриева // Gufo.me. – URL: https://gufo.me/dict/dmitriev (дата обращения: 01.04.2020).

18. ФинЦЕРТ // Банк России. – URL: https://cbr.ru/information_security/fincert (дата обращения: 23.04.2020).

19. Что такое хакинг и как от него обезопасить свой компьютер? // ProComputer.su. – URL: http://procomputer.su/comp-gramotnost/164-chto-takoe-khaking-i-kak-obezopasit-kompyuter (дата обращения: 09.04.2020).

20. Япония признала криптовалюты законным платежным средством // Российская газета. – URL: https://rg.ru/2017/04/01/iaponiia-priznala-kriptovaliuty-zakonnym-platezhnym-sredstvom.html (дата обращения: 14.03.2019).

21. ‘Zoom-bombing’ on the rise: Hijackers invade videoconferences for work, school, FBI says // The Mercury News. – URL: https://www.mercurynews.com/2020/03/31/coronavirus-zoom-bombing-hijackers-videoconferences (дата обращения: 27.02.2021).

22. 11 правил сетевой безопасности: как защититься от кибермошенников // Милосердие.ru. – URL: https://www.miloserdie.ru/article/11-pravil-setevoj-gigieny-kak-zashhititsya-ot-kiberprestupnosti (дата обращения: 27.02.2021).

23. Basel Committee on Banking Supervision Consultative Document Sound Practices: Implications of fintech developments for banks and bank supervisors: Issued for comment by 31 October 2017 // Bank for International Settlements. – URL: https://www.bis.org/bcbs/publ/d415.pdf (дата обращения: 13.12.2019).

24. Bitcoin.org. – URL: https://bitcoin.org (дата обращения: 05.02.2019).

25. Brazil – Supreme Court // Brazil Court. – URL: http://www.v-brazil.com/government/judiciary-branch/supreme-court.html (дата обращения: 23.04.2020).

26. Porn and Predators: Activists Warn of Internet Dangers for Kids During Coronavirus Crisis // Daily Caller. – URL: https://dailycaller.com/2020/03/28/porn-predators-internet-coronaviruschildren (дата обращения: 27.02.2021).

27. Report: WhatsApp has seen a 40 % increase in usage due to COVID-19 pandemic // TechCrunch. – URL: https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19pandemic (дата обращения: 27.02.2021).

28. Virtual currency schemes – a further analysis // European Central Bank. – URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (дата обращения: 14.12.2019).

ПРИЛОЖЕНИЯ

Приложение 1

Перечень вопросов судебной компьютерно-технической экспертизы[1]

1. *Вопросы, относящиеся к аппаратным средствам и решаемые с использованием методик производства КТЭ, направленных на решение диагностических задач*:

– какой тип, марку, модель, конфигурацию и технические характеристики имеет представленный объект?

– позволяет ли представленная компьютерная система решить функциональные задачи (указывается перечень задач)?

– находится ли представленный на экспертизу объект в рабочем состоянии?

– какие неисправности имеются в работе представленного на экспертизу объекта?

– присутствуют ли признаки, свидетельствующие о нарушении правил эксплуатации объекта?

– когда было подключено данное (указывается тип устройства) устройство к системному блоку, когда были установлены (инсталлированы) программы, обеспечивающие возможность (указываются возможности, например «распечатка машинограмм»)?

2. *Вопросы, относящиеся к программным средствам и решаемые с использованием методик производства КТЭ, направленных на решение диагностических задач*:

---

[1] Смолина А. Р. Методологическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы : дис. … канд. техн. наук : 05.13.19. Томск, 2017. С. 123–128. Вопросы приводятся в авторской редакции, некоторые из них представляются весьма спорными. Важно помнить! Представленные перечни вопросов являются лишь примерами формулировок. Круг же вопросов определяется исходя из конкретных обстоятельств дела и задач, стоящих перед следствием.

– какова общая характеристика объекта, представленного на экспертизу, каковы его компоненты (модули)?

– каковы наименование, версия, тип, вид представления (скрытый, явный, удаленный) программного обеспечения?

– каков состав компонентов программного обеспечения, представленного на экспертизу? Определение их характеристик (даты создания, объемы, атрибуты);

– каково функциональное предназначение программного средства?

– имеется ли на объекте, представленном на экспертизу, программное обеспечение, позволяющее реализовать определенную функциональную задачу?

– каковы требования, предъявляемые данным программным обеспечением к аппаратному программному обеспечению?

– совместимо ли данное программное обеспечение с аппаратно-программным обеспечением (указываются конкретные характеристики)?

– какова работоспособность программного обеспечения по реализации отдельных (конкретных) функциональных требований?

– каким образом выполняется операция или функция (указывается конкретно) в представленном на экспертизу программном обеспечении?

– имеет ли программное обеспечение отличия от предоставленного сравнительного образца? Если да, то какие?

– каков способ организации защиты информации на представленном объекте?

– каков алгоритм работы представленного на экспертизу программного обеспечения?

– каковы программно-инструментальные средства, использованные для разработки представленного на экспертизу программного обеспечения?

– позволяют ли изменения, внесенные в программное обеспечение, преодолеть его защиту?

– каков способ внесения изменений в программу (воздействие вредоносной программы, преднамеренное воздействие, аппаратный сбой, ошибка программной среды)?

– какова последовательность изменений в программном обеспечении?

– какова история использования программного обеспечения с момента его установки (либо за определенный промежуток времени)?

3. *Вопросы, относящиеся к данным компьютерной информации и решаемые с использованием методик производства КТЭ, направленных на решение диагностических задач*:

– каким образом было выполнено форматирование объекта? В каком виде записаны данные на него?

– какие характеристики имеет физическое размещение данных на представленном на экспертизе объекте?

– каковы характеристики логического размещения данных на объекте, представленном на экспертизу?

– каковы характеристики, свойства, параметры данных, содержащихся на объекте, представленном на экспертизу?

– каков вид информации на объекте, представленном на экспертизу (явный, скрытый, удаленный)?

– каков тип доступа к информации на объекте, представленном на экспертизу (свободный, ограниченный и пр.), и каковы его характеристики?

– каковы свойства и параметры средств защиты информации, каковы возможные пути их преодоления?

– каковы признаки преодоления защиты содержатся на объекте, представленном на экспертизу?

– каково содержание защищенной (зашифрованной) информации?

– каким образом выполнено действие (указывается какое)?

– какова последовательность действий по выполнению конкретной задачи? Каковы признаки ее выполнения?

– имеется ли зависимость (связь) между действиями (указывается перечень действий) и событием (указывается событие)?

4. *Вопросы, относящиеся к вычислительным сетям и их элементам и решаемые с использованием методик производства КТЭ, направленных на решение диагностических задач*:

– каковы свойства и характеристики аппаратного средства и программного обеспечения?

– каковы место, роль и функциональные предназначения исследуемого объекта в сети?

– каковы свойства и характеристики вычислительной сети, ее архитектура, конфигурация?

– какова организация доступа к данным?

– каково фактическое состояния сетевого средства, имеется ли наличие физических дефектов, каково состояние системного журнала, каков компонент управления доступом?

– какова причина изменения свойств вычислительной сети?

– какова структура механизмов и обстоятельств события (указывается перечень) в сети?

5. *Вопросы, относящиеся к аппаратным средствам и решаемые с использованием методик производства КТЭ, направленных на решение классификационных задач*:

– относится ли представленный на экспертизу объект к компьютерным средствам или их компонентам?

– каковы технические характеристики представленного на экспертизу объекта?

6. *Вопросы, относящиеся к программным средствам и решаемые с использованием методик производства КТЭ, направленных на решение классификационных задач*:

– к какому классу программного обеспечения относится представленный на экспертизу объект?

– относится ли представленный на экспертизу объект к классу (указывается класс)?

7. *Вопросы, относящиеся к данным компьютерной информации и решаемые с использованием методик производства КТЭ, направленных на решение классификационных задач*:

– каков тип данных, обнаруженных в результате производства экспертизы (графические, текстовые, данные ПЗУ, электронная таблица, запись пластиковой карты, база данных, мультимедиа и др.), с помощью какого программного обеспечения осуществляется работа с ними?

8. *Вопросы, относящиеся к вычислительным сетям и их элементам и решаемые с использованием методик производства КТЭ, направленных на решение классификационных задач*:

– к какому классу сетевых средств относится объект экспертизы?

– к какой части программного обеспечения относится объект экспертизы (серверной или клиентской)?

9. *Вопросы, относящиеся к аппаратным средствам и решаемые с использованием методик производства КТЭ, направленных на решение идентификационных задач*:

– какое (указывается тип устройства, например «знакопечатающее») устройство было подключено к представленному на исследование системному блоку, каковы его модель, серийный номер и т. п.?

10. *Вопросы, относящиеся к программным средствам и решаемые с использованием методик производства КТЭ, направленных на решение идентификационных задач*:

– каковы версия и наименование программного обеспечения?

– содержится ли на представленном на экспертизу объекте программное обеспечение, являющееся копией (название программы)? Идентифицирующий образец программы прилагается;

11. *Вопросы, относящиеся к данным компьютерной информации и решаемые с использованием методик производства КТЭ, направленных на решение идентификационных задач*:

– каковы данные с фактами и обстоятельствами по рассматриваемому делу, содержащиеся на представленном объекте?

– каковы пользовательские данные, содержащиеся на представленном на экспертизу объекте?

12. *Вопросы, относящиеся к вычислительным сетям и их элементам и решаемые с использованием методик производства КТЭ, направленных на решение идентификационных задач*:

– возможно ли идентифицировать отправителя электронного сообщения (режим доступа к сообщению регламентируется)?

– кем и каким образом была осуществлена транзакция денежных средств на сервисе (название сервиса, например, «Сбербанк Онлайн»)?

Типовые вопросы компьютерной экспертизы[1]

1. Следы работы какого аппаратного комплекса присутствуют в программном обеспечении НЖМД представленного системного блока ПК?

2. Соответствует ли конфигурация аппаратных средств, зафиксированная в информационной среде на НЖМД системных блоков, содержимому представленных системных блоков?

3. Имеются ли на накопителе на жестких магнитных дисках экземпляры программы Microsoft Office? Если да, то какова версия этой программы и иные данные, позволяющие идентифицировать программу; каковы обстоятельства установки и использования обнаруженных экземпляров программы?

---

[1] Рекомендации по изъятию компьютерной техники и носителей информации при проведении обыска. Варианты описания объектов, содержащих компьютерную информацию. С. 12–13.

Вопросы приводятся в авторской редакции.

4. Применяются ли при установке и эксплуатации программы Microsoft Office технические средства защиты авторских прав? Если да, то какие именно средства?

5. Если экземпляры программы Microsoft Office обнаружены, то выполнялись ли в ходе их установки и (или) использования действия, в результате которых стало невозможным использование технических средств защиты авторских прав либо эти технические средства перестали обеспечивать надлежащую защиту указанных прав? Какие именно действия такого рода выполнялись?

6. Если экземпляры программы Microsoft Office обнаружены, то установлены ли эти экземпляры программы способом, предусмотренным правообладателем?

7. Имеются ли на накопителе на жестких магнитных дисках сведения о подключении и использовании сетевого оборудования для обеспечения работы пользователя в сети «Интернет»?

8. Какие логины и пароли пользователь использовал для подключения к оборудованию провайдера и работы в сети «Интернет»?

9. В какие временные интервалы пользователь был подключен к провайдеру и мог работать в сети «Интернет»?

10. Имеются ли в файлах на накопителе на жестких магнитных дисках сведения о логинах и паролях иных пользователей?

11. Имеются ли на накопителе на жестких магнитных дисках программы, детектируемые как вредоносные? Если да, то имеются ли следы использования указанных программ?

12. Имеются ли на накопителе на жестких магнитных дисках программы обмена сообщениями? Если да, то каковы реквизиты отправителя и адресатов сообщений?

13. Имеются ли среди сообщений сообщения, относящиеся тематически к обсуждению проблем подготовки, осуществления несанкционированных подключений к сетевым компьютерам,

использования логинов и паролей пользователей, осуществления иных действий деструктивного характера? Каковы реквизиты этих сообщений?

14. Присутствует ли в представленных базах данных сведения об изготовлении платежного поручения № ___ от дд.мм.гггг.

15. Каковы обстоятельства создания и изготовления документа?

16. Возможно ли изготовление представленного документа с использованием представленной компьютерной техники? Если да, то присутствуют ли в памяти представленного компьютера следы изготовления документа?

Типовые вопросы комплексной судебной видеотехнической и компьютерно-технической экспертизы[1]

1. Каков формат записи, содержащейся на представленном носителе?

2. Содержит ли представленная видеозапись признаки монтажа?

3. Является ли представленная видеозапись копией или оригиналом?

4. Какого размера предметы находятся в пространстве кадра?

5. Какой вид, тип или марка устройства использовалась для изготовления исследуемой видеозаписи?

6. Были ли стерты какие-либо части представленной видеозаписи?

[1] Воронкова Д. К., Воронков А. С., Пилипчак А. М. Комплексная судебная компьютерно-техническая и видеотехническая экспертиза // Modern Science. 2019. № 12-1. С. 300–306.

Вопросы приводятся в авторской редакции.

Приложение 2

Основные проблемы обеспечения процессуальных действий в банке и распространенные ошибки со стороны сотрудников МВД России, направляющих (предоставляющих) в подразделения банка постановления, запросы и иные процессуальные документы для исполнения

Поступление в банк постановлений, запросов и иных процессуальных документов для исполнения осуществляется посредством Почты России, через официальный адрес электронной почты www.sberbank.ru и при личном обращении сотрудника правоохранительного органа (далее по тексту – ПХО) в подразделения банка.

При личном обращении сотрудника ПХО в банк для передачи в работу постановлений, запросов и иных процессуальных документов, а также для проведения следственных действий и оперативно-разыскных мероприятий осуществляется вызов сотрудника подразделения безопасности (далее по тексту – ПБ). Сотрудник ПБ проверяет и переписывает реквизиты служебного удостоверения сотрудника ПХО, сверяет фото на служебном удостоверении с личностью предъявителя, проверяет правильность составления и оформления процессуальных документов (его реквизиты, форму и содержание на наличие существенных технических ошибок, исправлений, подчисток и т. д.).

1. Порядок обеспечения производства выемки предметов, документов

При личном обращении сотрудника ПХО в банк с постановлением о производстве выемки или при получении его по Почте России сотрудник ПБ осуществляет запрос подлежащих изъятию документов, предметов в подразделение банка, ответственное за их хранение, после чего осуществляет выдачу материалов сотруднику ПХО, который составляет протокол и вносит в него перечень изъятых документов, предметов. Копия протокола по окончании

следственного действия вручается представителю банка (руководителю подразделения, в котором проводилось следственное действие, либо сотруднику ПБ) под расписку в протоколе.

2. Порядок обеспечения производства обыска в помещениях банка

При производстве обыска сотрудники ПХО лично обращаются в подразделения банка с постановлением о производстве обыска. На место прибытия сотрудников ПХО вызывается сотрудник ПБ для организации производства обыска.

В случае выявления существенных ошибок в предъявленном постановлении сотрудник ПБ информирует сотрудника ПХО о несогласии с производством обыска или невозможности его производства, о чем делается отметка в протоколе обыска (в случае его составления), либо готовит мотивированный ответ за подписью соответствующего руководителя банка или лица, уполномоченного на подписание соответствующих документов.

Обыск производится в помещении банка, указанном в предъявленном постановлении, с участием сотрудников банка, в том числе сотрудника ПБ. В случае изъятия электронных носителей информации со стороны банка может привлекаться специалист. При производстве обыска может проводиться фото- и видеосъемка, могут составляться планы и схемы. В процессе производства обыска в помещениях подразделений банка осуществляется изъятие предметов и документов, указанных в постановлении о производстве обыска.

По результатам проведения обыска сотрудник правоохранительных органов составляет протокол и вносит в него перечень изъятых документов. В протокол могут вноситься замечания участвующими лицами (в том числе о нарушении прав клиентов, банка, его работников, иных лиц). Протокол подписывается сотрудником ПХО и участвующими лицами (руководителем подразделения, в помещении которого производится обыск, понятыми и др.).

3. Порядок обеспечения производства осмотра места происшествия, предметов, документов в помещениях и на территории банка

При личном обращении сотрудника ПХО в подразделение банка с необходимостью производства осмотра вызывается сотрудник ПБ. При отсутствии явных оснований для проведения осмотра (отсутствие события преступления на территории банка, отсутствие процессуальных полномочий у сотрудника ПХО, явная нецелесообразность осмотра и др.) сотрудник ПБ сообщает о своих замечаниях сотруднику ПХО и требует их внесения в протокол осмотра, после его проведения снимая с протокола копию для обжалования.

Осмотр места происшествия может проводиться в помещениях (на территории) банка по преступлениям, произошедшим непосредственно в его помещениях (на территории).

Производство осмотра места происшествия осуществляется с участием руководителя (заместителя руководителя) подразделения банка, в помещении (на территории) которого производится осмотр, в присутствии сотрудника ПБ. По усмотрению сотрудника ПХО к участию в осмотре со стороны банка может привлекаться специалист. При производстве осмотра может проводиться фото- и видеосъемка, могут проводиться измерения, составляться планы и схемы. В ходе осмотра могут изыматься:

– следы преступления и предметы со следами преступления;

– предметы, послужившие орудием преступления, а также предметы, на которые были направлены преступные действия;

– электронные носители информации;

– денежные средства, ценности и иное имущество, полученное в результате совершения преступления;

– предметы, запрещенные к обращению;

– документы, являющиеся вещественными доказательствами.

Осмотр предметов, документов может производиться в помещении банка непосредственно после их изъятия в ходе проведения других следственных действий (выемки, обыска).

По окончании производства осмотра сотрудник ПХО составляет протокол, который подписывается сотрудником ПХО и участвующими лицами (руководителем подразделения, в помещении которого производится осмотр, понятыми и др.). В протоколе сотрудник ПХО указывает перечень изъятых предметов, документов (при изъятии), участниками осмотра могут вноситься замечания (в том числе о нарушении прав клиентов, банка, его работников, иных лиц). С разрешения сотрудника ПХО сотрудник ПБ снимает копию с протокола для подтверждения произведенного осмотра, которую в тот же день передает в подразделение, где производился осмотр.

4. Особенности наложения ареста на денежные средства и иное имущество клиентов банка

Предъявленное в банк сотрудниками ПХО постановление о наложении ареста на ценные бумаги, изъятые в ходе досудебного производства по уголовным делам и не находящиеся на хранении в банке, должно содержать конкретную информацию о том, что ценные бумаги, подлежащие аресту, были изъяты органами предварительного расследования (Ф. И. О лица, у которого изъяты ценные бумаги, их вид, серия и номер, номинальная стоимость, дата выпуска).

Арест, наложенный на имущество, отменяется на основании постановления следователя (дознавателя), в производстве которого находится уголовное дело, а также в случае истечения срока ареста, наложенного на имущество, или отказа в его продлении судом в соответствии с ч. 9 ст. 115 УПК РФ. Порядок продления ареста на имущество осуществляется в соответствии со ст. 115.1 УПК РФ.

5. Поступающие в банк запросы о предоставлении информации в отношении счетов и операций клиентов банка

Относится также и к запросам следователей с согласия руководителя следственного органа, постановлениям судов о проведении оперативно-разыскного мероприятия «наведение справок».

Запросы направляются для рассмотрения в соответствующий Региональный центр сопровождения банковских операций г. Самары и г. Нижний-Новгород.

Запросы, касающиеся иной информации банка (в отношении работников, банковских процессов и продуктов и т. д.), направляются в подразделения банка, в компетенции которых находится тот или иной процесс.

Самые распространенные ошибки сотрудников ПХО при предъявлении постановлений, решений судов, запросов для проведения следственных (процессуальных) действий и оперативно-разыскных мероприятий в банке, влекущие неисполнение требований:

– в постановлениях следователя, суда о производстве следственных действий, оперативно-разыскных мероприятий неправильно указаны адрес, место проведения следственного действия;

– в постановлениях следователя, суда о производстве следственных действий, оперативно-разыскных мероприятий неправильно указаны данные юридического (физического) лица, в отношении которого необходимо проведение следственных действий, оперативно-разыскных мероприятий;

– в случае поступления в банк запроса о предоставлении информации, составляющей банковскую тайну, без судебного решения, когда такое решение обязательно в соответствии со ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности», такой запрос не подлежит исполнению с соответствующим ответом инициатору запроса;

– в банк может поступить обращение о предоставлении информации со ссылкой, что имеется судебное решение, но оно не приложено к обращению;

– в запросе ПХО имеется требование о направлении ответа в его адрес по незащищенной электронной почте;

– в случае поступления в Банк постановления суда о разрешении производства выемки с сопроводительным письмом, в котором содержится информация о предоставлении документов по адресу нахождения ОМВД, УМВД либо по факсу, данные требования незаконны, поскольку на основании суда о разрешении производства выемки необходимо изъятие данных документов и информации с составлением протокола выемки в соответствии с требованиями УПК РФ;

– постановлением о снятии ареста с денежных средств, признании их вещественными доказательствами по уголовному делу и о передаче их третьему лицу и другие требования, которые банком не могут быть выполнены в силу нарушения норм действующего законодательства.

Приложение 3

Образцы запросов в банк

Руководителю ПАО «N»

(реквизиты)

на № _____ от _____

О предоставлении сведений
по уголовному делу № *****

Уважаемый XXX!

В производстве XXX находится уголовное дело № *****, возбужденное 19.05.2016 по признакам преступления, предусмотренного пп. «в», «г» ч. 3 ст. 158 УК РФ, по факту хищения неустановленными лицами денежных средств в крупном размере на сумму 500 тыс. руб. у Ивановой Тамары Михайловны, 25 апреля 1956 года рождения.

Руководствуясь ст.ст. 21, 38, 73, 74 и 86 УПК РФ, ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» (в ред. от 27.12.2019), прошу предоставить сведения обо всех счетах, открытых (открывавшихся ранее) в ПАО «N» на имя физических лиц согласно нижеприведенному списку:

ФИО	Дата рождения	Гражданство	Паспорт (виза)

Одновременно прошу предоставить выписки о движении денежных средств по указанным счетам с момента их открытия до настоящего времени.

Старший следователь
по особо важным делам _____

СОГЛАСОВАНО
Руководитель следственного органа _____

Руководителю ПАО «N»

(реквизиты)

на № _____ от _____

О предоставлении сведений
по уголовному делу № *****

В производстве Н. находится уголовное дело № *******, возбужденное 02.02.2017 по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ, по факту хищения денежных средств в сумме ** *** руб. у Самарцевой Галины Павловны, 03 марта 1972 года рождения.

Руководствуясь ст.ст. 21, 38, 73, 74 и 86 УПК РФ, ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» (в ред. от 27.12.2019), прошу Вас предоставить:

1. Выписку о движении денежных средств по расчетным счетам № NNN и № NNN, открытым на имя XXX за период с 01.01.20** по 01.03.20**, с обязательным указанием в выписках:

1) номера расчетного счета;
2) входящего остатка;
3) даты операции;
4) номера документа;
5) плательщика;
6) получателя;
7) суммы по дебету (рубли, копейки) (расход);

8) суммы по кредиту (рубли, копейки) (приход);
9) назначения платежа;
10) итого оборотов по дебету (рубли, копейки);
11) итого оборотов по кредиту (рубли, копейки).

Прошу указать по всем расчетным счетам информацию о доверенных лицах (при наличии) на право совершения операций, получения выписок и платежных документов, совершения операций с ценными бумагами с обязательным указанием установочных данных лиц, обозначенных в доверенности, даты оформления доверенности, срока действия доверенности, Ф. И. О. нотариуса, а также сведения о заключении договора на использование системы ДБО. При проведении операций с использованием ДБО предоставить выписку IP-адресов в период с **.**.20** по **.**.20**).

2. В случае приобретения указанными выше по тексту лицами векселей банка в период с 01.01.20** по 01.03.20** прошу предоставить копии договоров купли-продажи векселей, актов приема-передачи векселей, копии векселей, копии актов приема-передачи векселей последними векселедержателями. В случае предъявления лицами, указанными выше, векселей банка к погашению с 01.01.20** по 01.03.20**, прошу предоставить копии заявлений на погашение векселей, актов приема-передачи векселей, копии векселей (с индоссаментами), копий актов приема-передачи векселей первым векселедержателям.

Следователь_____

СОГЛАСОВАНО
Руководитель следственного органа _____

Руководителю ПАО «N»

(реквизиты)

_____ № _____

на № _____ от _____

О предоставлении сведений
по уголовному делу № *****

В производстве Н. находится уголовное дело № *****, возбужденное 19.05.2016 по признакам преступления, предусмотренного п. «б» ч. 2 ст. 171 УК РФ. Руководствуясь ст.ст. 21, 38, 73, 74 и 86 УПК РФ, ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» (в ред. от 27.12.2019), прошу Вас предоставить сведения за период с 13.07.20** по 15.07.20** в отношении указанных ниже юридических лиц:

1. Арбитражный управляющий ООО «N», ИНН XXX.
2. ООО «XXX», ИНН XXX.

При наличии информации на указанных юридических лиц необходимо предоставить следующие сведения:

1. О наличии открытых счетов, движении и остатке денежных средств по расчетным счетам с обязательным указанием следующих реквизитов: номера и даты совершения операций, номера и даты платежного документа, основания перечисления денежных средств, реквизитов плательщика

(получателя) денежных средств, ИНН плательщика (получателя) денежных средств.

2. Об обращении в кредитную организацию за получением кредита, а также заложенном имуществе по данному кредиту.

3. О приобретении векселей, ценных бумаг, драгоценных металлов, о заключении договора аренды банковской ячейки (для физических лиц).

4. Содержащиеся в карточках с образцами подписей и оттисками печати, в том числе ранее аннулированных клиентом, с обязательным указанием установочных данных лиц, обозначенных в карточке (Ф. И. О, должностное положение), нотариуса, заверившего карточку, даты оформления карточки, регистрационного номера реестра нотариальных действий, в который внесена соответствующая запись (для юридических лиц).

5. О лицах, с которыми заключены договоры на обслуживание расчетных счетов с использованием систем «клиент-банк», «интернет-банк», сведения об удаленном доступе по управлению расчетными счетами с указанием адреса, лог-файла, а также иных идентификационных данных пользователя с обязательным приложением заверенных копий документов, подтверждающих эти сведения;

6. Об IP-адресах, используемых для проведения операций по расчетным счетам с обязательным указанием реквизитов.

С уважением,
Следователь _____

СОГЛАСОВАНО
Руководитель следственного органа _____

Образец запроса на получение информации о наличии счетов юридического лица по возбужденному уголовному делу

М И Н И С Т Е Р С Т В О
ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МВД России)

Руководителю ПАО «N»

(реквизиты)

_____ № _____
на № _____ от _____

О представлении сведений
по уголовному делу № *****

В производстве Н. находится уголовное дело № *****, возбужденное **.**.20** по признакам преступления, предусмотренного ч. * ст. 1** УК РФ, по факту хищения денежных средств в сумме ***** руб. у ООО «N.» (сокращенное наименование организации), ИНН ********.

На основании вышеизложенного и руководствуясь ст.ст. 21, 38, 73, 74 и 86 УПК РФ, ст. 26 Федерального закона от 02.12.1990 № 395-I «О банках и банковской деятельности» (ред. от 27.12.2019), прошу Вас предоставить следующие сведения, в том числе на электронном носителе, о наличии счетов юридического лица (индивидуального предпринимателя) по следующим реквизитам:

ИНН _____;

сокращенное наименование организации _____
_____;

ФИО ИП _____, _____ г.р., паспорт_____, –

следующие данные:

– наименование ВСП, где открыт счет;
– номер счета;
– вид счета;
– валюта счета;
– дата открытия счета;
– дата закрытия счета;
– номер корпоративной карты;
– Ф. И. О. держателя корпоративной карты.

Полные сведения об остатках на счетах юридического лица (индивидуального предпринимателя) по следующим реквизитам:

ИНН _____;

сокращенное наименование организации _____ _____;

ФИО ИП _____, _____ г.р., паспорт _____;

номер счета _____, – по состоянию на _____ г.

Могут быть представлены следующие данные:

– наименование ВСП, где открыт счет;
– номер счета;
– вид счета;
– номер счета;
– валюта счета;
– дата, на которую требуется остаток;
– дата открытия счета;
– дата закрытия счета;
– входящий остаток на дату;
– статус счета;
– дата открытия счета;
– дата закрытия счета.

Предоставление информации по ценным бумагам, векселям, сертификатам юридического лица (индивидуального предпринимателя) по следующим реквизитам:

ИНН _____;

сокращенное наименование организации _____ _____;

ФИО ИП _____, _____ г.р., паспорт _____;

серия и номер сертификата (векселя) _____ _____, – за период с_____ по _____г.

Могут быть представлены следующие данные:

- серия векселя (сертификата);
- номер векселя (сертификата);
- валюта векселя (сертификата);
- ставка сертификата;
- дата выдачи;
- Ф. И. О. первого держателя;
- ДУЛ;
- сумма начисленной оплаты;
- Ф. И. О. последнего держателя;
- ДУЛ;
- наименование организации;
- ИНН;
- сумма;
- статус оплаты;
- дата оплаты векселя;
- кем оплачен (Ф. И. О.);
- ДУЛ;
- кем оплачен (наименование организации);
- ИНН;
- место оплаты.

Полная выписка по счетам юридического лица (индивидуального предпринимателя) по следующим реквизитам:

ИНН _____;

сокращенное наименование организации _____ _____;

ФИО ИП _____, _____ г.р., паспорт _____;

счет № _____, – за период с_____ по _____ г.

Могут быть представлены следующие данные:

– наименование ВСП, где открыт счет;
– номер счета;
– вид счета;
– валюта счета;
– дата открытия счета;
– дата закрытия счета;
– статус счета;
– входящий остаток на дату;
– операции по дебету;
– операции по кредиту;
– назначение;
– исходящий остаток.

Ответ прошу направить посредством электронного документооборота.

Заранее благодарим за сотрудничество!

Следователь _____

СОГЛАСОВАНО
Руководитель
следственного органа _____

Образец запроса на получение информации по возбужденному уголовному делу

М И Н И С Т Е Р С Т В О
ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МВД России)

Руководителю ПАО «N»

(реквизиты)

_____ № _____
на № _____ от _____

О представлении сведений
по уголовному делу № *****

В производстве Н. находится уголовное дело № *****, возбужденное **.**.20** по признакам преступления, предусмотренного ч. * ст. 1** УК РФ, по факту хищения денежных средств в сумме ***** руб. у ООО «N.» (сокращенное наименование организации), ИНН ********.

В настоящее время в целях полного, всестороннего и объективного расследования, а также установления всех обстоятельств совершения преступления требуется получение сведений по счету ООО «N.», ИНН ********, № **********, открытому в Вашем банке, по состоянию на _____ г.

На основании вышеизложенного и руководствуясь ст.ст. 21, 38, 73, 74 и 86 УПК РФ, ст. 26 Федерального закона от 02.12.1990 № 395-I «О банках и банковской деятельности» (ред. от 27.12.2019), прошу Вас предоставить следующие сведения, в том числе на электронном носителе, а именно:

- наименование ВСП, где открыт счет;
- номер счета;
- вид счета;
- номер счета;
- валюта счета;

- дата открытия счета;
- дата закрытия счета;
- входящий остаток на дату;
- статус счета.

Заранее благодарим за сотрудничество!

Следователь _____

СОГЛАСОВАНО
Руководитель
следственного органа _____

Образец запроса на получение информации при проведении доследственной проверки

М И Н И С Т Е Р С Т В О
ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МВД России)
_____ № _____
на № _____ от _____

Руководителю ПАО «N»

(реквизиты)

О предоставлении сведений

В связи с проведением проверки по сообщению о преступлении, зарегистрированном в КУСП №_____ от 21.02.2018 по заявлению Ф. И. О, 03.12.1956 года рождения, ДУЛ № ******, по факту проведения неправомерных операций в сумме **** руб. 20.02.2018, руководствуясь ч. 4 ст. 10, п. 4 ч. 1 ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» (с последними изменениями от 06.02.2020), просим Вас предоставить в наш адрес сведения об IMEI телефонов и IP-адресах устройств, с помощью которых осуществлялись хищения денежных средств в период с ____ _____ 20____ г. по ____ _____ 20____ г.

Ответ прошу направить посредством электронного документооборота.

Заранее благодарим за сотрудничество!

Следователь _____

Образец запроса на получение информации в связи с проведением ОРМ

М И Н И С Т Е Р С Т В О
ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МВД России)

Руководителю ПАО «N»

(реквизиты)

_____ № _____
на № _____ от _____

О представлении сведений

В связи с возникшей необходимостью и проводимыми оперативно-розыскными мероприятиями, руководствуясь ч. 4 ст. 10, чч. 1, 4 ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» (с последними изменениями от 06.02.2020), ст.ст. 6–8 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (с последними изменениями от 02.08.2019), прошу Вас предоставить следующие сведения:

– место выдачи банковской карты (номер карты);

– информация о привязке абонентских номеров к указанной банковской карте;

– способ перевода денежных средств;

– адрес места перевода денежных средств;

– реквизиты получателя денежных средств;

– адрес места обналичивания денежных средств;

– сведения об IP-адресах, с которых осуществлялся вход в систему удаленного доступа в период с ____ _____ 20____г. по ____ _____ 20____г.;

– информация о других клиентах, у которых осуществлялся вход в систему удаленного доступа с этого же IP-адреса, и IMEI устройств.

Просим Вас принять меры к сохранению видеофиксации в УС банка, в которых проводилось обналичивание похищенных денежных средств в период с ____ _____ 20____г. по ____ _____ 20____г., предоставить фотофиксацию лица, которое осуществляло снятие денежных средств по вышеуказанной карте в период с ____ _____ 20____г. по ____ _____ 20____г., для проведения дальнейшей идентификации лица, проводившего данную операцию.

Следователь _____

Образец сопроводительного письма к постановлению судьи на получение информации «наведение справок» во исполнение постановления судьи

М И Н И С Т Е Р С Т В О
ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МВД России)

Руководителю ПАО «N»

(реквизиты)

_____ № _____
на № _____ от _____

О представлении сведений
по судебному решению

В связи с возникшей необходимостью и проводимыми оперативно-розыскными мероприятиями, руководствуясь ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» (с последними изменениями от 06.02.2020), ст. 6 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (с последними изменениями от 02.08.2019), а также на основании постановления судьи Н. районного суда г. Н. (Ф. И. О. судьи) (№ постановления, от дд.мм.гггг) прошу Вас предоставить:

– информацию о полных анкетных данных и контактных телефонах лиц, на которые открыты банковские карты и счета, номера карты, номера счета;

– информацию о движении денежных средств по указанным банковским картам и счетам с указанием имеющихся реквизитов поступления и снятия денежных средств, номеров и адресов отделений (банкоматов), в которых осуществлялась выдача денежных средств в период с ____ _____ 20____г. по ____ _____ 20____г.;

– информацию об используемых IP-адресах, IMEI устройств и других сетевых реквизитах, используемых для подключения посредством сети «Интернет» к системе дистанционного обслуживания указанных банковских карт и счетов за период с ____ _____ 20 ____ г. по ____ _____ 20 ____ г.

Приложение: постановление судьи на ___ листах.

Следователь _____

Учебное издание

Гончар Владимир Владимирович,
кандидат юридических наук, доцент

Молчанова Татьяна Витальевна,
кандидат юридических наук, доцент

Шмарион Полина Вячеславовна,
кандидат юридических наук

Шаров Александр Васильевич,
кандидат юридических наук, доцент

Медведева Мария Олеговна,
кандидат юридических наук

Дайшутов Михаил Михайлович,
кандидат юридических наук, доцент

Русскевич Евгений Александрович,
кандидат юридических наук

Горач Николай Николаевич,
кандидат педагогических наук

Химичева Ольга Викторовна,
доктор юридических наук, профессор

Тумаков Альберт Вячеславович,
кандидат юридических наук

Андреев Алексей Владимирович,
кандидат юридических наук

Стащенко Станислав Петрович,
кандидат юридических наук

Джафарова Найля Тахировна

Долбилов Алексей Владимирович,
кандидат экономических наук

Любан Владислав Григорьевич,
кандидат юридических наук, доцент

Иванов Дмитрий Александрович,
доктор юридических наук, доцент

Михайленко Наталья Васильевна,
кандидат юридических наук, доцент

Клишина Наталья Егоровна

Гусев Дмитрий Владимирович

Смирнов Игорь Владимирович

Савенкова Дарья Дмитриевна,
кандидат юридических наук

Захаров Дмитрий Никанорович,
кандидат технических наук

Завьялов Максим Валерьевич

Тарасов Дмитрий Александрович

Противодействие преступлениям в сфере информационных технологий

Редактор *Фомин И. Е.*, *Лосева О. С.*
Корректор *Фомин И. Е.*, *Лосева О. С.*
Компьютерная верстка *Лосева О. С.*

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12

Подписано в печать 27.10.2021	Формат 60×84 1/16	Тираж	284 экз.
Заказ № 92	Цена договорная	Объем	12,94 уч.-изд. л.
			19,29 усл. печ. л.