Министерство внутренних дел Российской Федерации
Казанский юридический институт

Н.Р. Шевко
А.М. Каримов
Е.Э. Турутина

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ

Учебное пособие

Казань 2017

ББК 32.81
Ш 31

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты

кандидат юридических наук Л.Б. Сыромля
(Владивостокский филиал Дальневосточного
юридического института МВД России)

доктор педагогических наук В.А. Горбунов
(ЧОУ ВО «Академия социального образования»)

Шевко Н.Р.

Ш 31 Преступления, совершаемые с использованием высоких технологий и коммуникаций : учебное пособие / Н.Р. Шевко, А.М. Каримов, Е.Э. Турутина. – Казань : КЮИ МВД России, 2017. – 80 с.

Учебное пособие направлено на формирование базовых знаний и навыков проведения расследования уголовных дел по преступлениям, совершаемым с использованием высоких технологий и коммуникаций.

Учебное пособие ориентировано на курсантов и слушателей образовательных организаций системы МВД России, подготовлено в соответствии с курсом «Расследование преступлений в сфере компьютерной информации и высоких технологий» и дополнительной программой повышения квалификации сотрудников следственных и экспертно-криминалистических подразделений, подразделений дознания, специально-технических мероприятий, уголовного розыска, по контролю за оборотом наркотиков, противодействию экстремизму, экономической безопасности и противодействию коррупции территориальных органов МВД России, осуществляющих функции по противодействию преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий.

ISBN 978-5-906977-02-1 **ББК 32.81**

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Продолжающееся стремительное развитие телекоммуникационных технологий напрямую отражается и на количестве преступлений, совершаемых в данной сфере. В настоящее время практически все виды преступлений могут совершаться с использованием телекоммуникаций и компьютерной информации. Подавляющее большинство преступлений в данной сфере связано с различными видами хищений, такими, как мошенничество. Не является исключением платежная система. Электронные платежи и средства расчета в точке продажи – примеры использования новых технологий, коренным образом меняющих финансовую индустрию.

Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации[1].

Средства телекоммуникаций и новые информационные технологии создают условия для подготовки, совершения и сокрытия хищений денежных средств с их использованием, к которым относятся: виртуальный характер дистанционных банковских операций; доступность открытых телекоммуникационных сис-

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

тем; высокая скорость выполнения транзакций; глобальный характер межсетевого операционного взаимодействия[1].

В большинстве случаев подобные преступления по своему характеру и механизму совершения являются однотипными. Средствами и орудиями их совершения могут являться как простейшие мобильные телефоны, так и средства связи с доступом в сеть Интернет. При этом сама сеть Интернет выступает в качестве своеобразной площадки, на которой мошенники реализуют свой преступный умысел. Преступники не только используют компьютерные технологии в своих целях, но и разрабатывают программные продукты (вредоносные и троянские программы) для облегчения подготовки, совершения и сокрытия таких хищений, новые методы (способы) компрометации банковских карт, персональных компьютеров, банковских автоматизированных систем, в том числе методы передачи скомпрометированной информации.

Возрастают масштабы компьютерной преступности, прежде всего, в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

Согласно данным аналитического обзора ФГКУ ВНИИ МВД России в 2917 году прогнозируется расширение присутствия преступности в виртуальном пространстве (киберпреступность). Наряду с совершением в интернет-сети традиционных видов преступных посягательств – краж денежных средств из электронных кошельков, банкоматов, с телефонных счетов, мошенничеств, в том числе так называемых телефонных, сбора и продажи конфи-

[1] Ревенков П.В. Управление рисками в условиях электронного банкинга: автореф. дис. ... д-ра эконом. наук. СПб., 2013. С. 20.

денциальной информации, вымогательств, возрастает число преступлений экстремистской направленности (+28,9%; 950) и террористического характера (+39,8%; 186), совершаемых с использованием сети Интернет, распространения через Интернет предметов и услуг, исключенных из легального оборота (наркотических средств, детской порнографии), а также использования киберсетей для организации преступной деятельности и сокрытия ее следов, особенно в сфере наиболее опасных видов преступности[1].

Статья 23 Доктрины информационной безопасности Российской Федерации определяет, что повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям является одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности[2].

В России в 2015 году в сфере телекоммуникаций и компьютерной информации было зарегистрировано 8446 краж и 13464 мошенничества[3]. Большинство таких преступлений совершается в кредитно-финансовой системе.

По данным председателя Сберегательного банка России Г. Грефа только сейчас в мире действует примерно 40 миллионов киберпреступников. 10 лет назад лишь два процента преступлений совершались с помощью киберсредств. Но сейчас ситуация изменилась кардинально[4]. Преступления в сфере компьютерной информации хотя и имеют незначительный удельный вес в об-

---

[1] Комплексный анализ состояния преступности в РФ по итогам 2016 года и ожидаемые тенденции ее развития: аналитический обзор. М.: ФГКУ ВНИИ МВД России, 2017.

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

[3] Представленные результаты получены на основе обобщения статистических данных ГИАЦ МВД России, содержащихся в форме отчетности 1 - ВТ (код. 615) «О преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации», утвержденной приказом МВД России от 1 апреля 2002 г. № 311.

[4] Греф: необходимо создать систему по борьбе с киберпреступниками. URL: http://ria.ru/economy/20160412714092152 02.html (дата обращения: 28 июля 2017).

щей структуре преступности, однако проявляют стойкую тенденцию к ежегодному росту.

Если раньше специфика преступлений в сфере компьютерной информации была обусловлена использованием при их совершении высоких технологий и новейших достижений науки и техники, необходимостью обладания определенным уровнем специальных познаний, то в настоящее время в глобальной сети Интернет в практически свободном доступе находятся как программы, предназначенные для совершения несанкционированных действий с компьютерной информацией, так и инструкции по их применению[1].

Как представляется, положительные результаты в расследовании хищений денежных средств, совершаемых с использованием компьютерной информации, могут быть достигнуты только при условии совместных и согласованных действий законодателя, органов исполнительной власти, в том числе правоохранительных, организаций банковской и платежных систем, коммерческих компаний, осуществляющих деятельность в сфере информационной безопасности, а также компетентных органов зарубежных государств.

Для раскрытия и расследования таких преступлений сотрудникам ОВД достаточно иметь доступ к сети Интернет и следовать определенному алгоритму действий, в основном, состоящему в направлении запросов на установление ряда технических параметров. В качестве проблемы необходимо обозначить, что деятельность по раскрытию и расследованию преступлений, совершаемых с использованием высоких технологий и коммуникаций, осуществляется сотрудниками ОВД в условиях отсутствия механизмов взаимодействия с банками, операторами сотовой связи, провайдерами.

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России). Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

В качестве проблемы отдельно стоит выделить отсутствие специалистов в сфере компьютерной информации, которые могли бы оказать содействие в расследовании такого рода преступлений, а также слабую программно-техническая оснащенность подразделений ОВД.

Оперуполномоченные, дознаватели и следователи, специализирующиеся на расследовании обозначенных преступлений, не обладают достаточным уровнем специальных познаний, навыков в соответствующей области профессиональной деятельности.

- ✓ Так, в ходе проведенного нами опроса[1] сотрудников МВД по РТ, было установлено, что лишь 4 процента опрошенных имеют профильное образование (в сфере информационных технологий), остальные респонденты имеют юридическое образование. Уровень владения персональным компьютером среди опрошенных:
- ✓ низкий (владею навыками работы в текстовом редакторе) – 26%,
- ✓ средний (могу переустановить ОС) – 69 %,
- ✓ высокий (владею навыками дизайна интернет-страниц, написания скриптов, программирования) – 5%.

Представляется, что настоящее учебное пособие будет способствовать повышению уровня профессиональной подготовки сотрудников ОВД, специализирующихся на пресечении, раскрытии и расследовании преступлений, совершаемых с использованием высоких технологий и телекоммуникаций.

[1] Опрос проводился среди сотрудников МВД по РТ, проходивших обучение по дополнительной программе повышения квалификации сотрудников следственных и экспертно-криминалистических подразделений, подразделений дознания, специально-технических мероприятий, уголовного розыска, по контролю за оборотом наркотиков, противодействию экстремизму, экономической безопасности и противодействию коррупции территориальных органов МВД России, осуществляющих функции по противодействию преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий, в образовательных организациях МВД России, расположенных по месту совместной дислокации. КЮИ МВД России, 2017 г.

Глава 1.
УГОЛОВНО-ПРАВОВАЯ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ

1.1. Понятие и виды преступлений, совершаемых с использованием высоких технологий и телекоммуникаций

Вопросы противодействия преступлениям в сфере высоких технологий невозможно рассматривать, предварительно не выделив объект и предмет исследования.

Высокие технологии (англ. high technology, high tech, hi-tech) – система знаний, производственных и иных операций, методов и процессов, соответствующая или превосходящая по своим качественным показателям мировые аналоги и позволяющая достигать показателей производительности труда высшего мирового уровня[1]. Это собирательное понятие и предполагает наиболее новые и прогрессивные технологии современности. К высоким технологиям в настоящее время относят самые наукоемкие отрасли промышленности.

Термином **«информационные технологии»** обозначают процессы, методы поиска, сбора, хранения, обработки, предос-

[1] О Концепции создания Евразийской инновационной системы: решение № 475 Межгосударственного Совета Евразийского экономического сообщества: принято в г. Санкт-Петербурге 11.12.2009. Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

тавления, распространения информации и способы осуществления таких процессов и методов[1].

В научных кругах наряду с правовой категорией «преступления, совершаемые с использованием высоких технологий и телекоммуникаций» часто употребляются термины «киберпреступность», «компьютерные преступления», «преступления в сфере компьютерной информации», «преступления в сфере высоких технологий» и т.д.

Киберпреступность – это любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети[2].

Компьютерное преступление как уголовно-правовое понятие — это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства.

В литературе обращается внимание на то, что эти термины очень близки друг другу, но все-таки не синонимичны. Понятие «киберпреступность» (в англоязычном варианте – cybercrime) шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого явления, как преступность в информационном пространстве.

В российском законодательстве, в частности в УК РФ, понятия «преступления, совершаемые с использованием высоких технологий и телекоммуникаций» и «киберпреступность» отсутствуют. В УК РФ обозначена глава 28 «Преступления в сфере ком-

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон РФ от 27.07.2006 № 149-ФЗ: ред. от 29.07.2017. Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

[2] Преступления, связанные с использованием компьютерной сети / Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями // A / CONF.187/10. Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

пьютерной информации», в которую включены общественно опасные деяния, предусмотренные ст. 272 «Неправомерный доступ к компьютерной информации»; 273 «Создание, использование и распространение вредоносных компьютерных программ»; 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации»[1].

Социологические исследования, проведенные среди практических работников (следователей, дознавателей), показали, что чаще всего им приходится расследовать следующие виды преступлений, совершаемых с использованием высоких технологий: мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), кража (ст. 158 УК РФ), неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ (ст. 242 УК РФ)[2].

Киберпреступность охватывает любое преступление, которое может быть совершено в электронной среде. Существуют две категории киберпреступлений:

- ✓ киберпреступление в узком смысле – любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных;
- ✓ киберпреступление в широком смысле – любое противоправное деяние, совершаемое посредством или в связи с компью-

[1] Уголовный кодекс Российской Федерации: Федеральный закон РФ от 13.06.1996 № 63-ФЗ: ред. от 18.07.2017. Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

[2] Опрос проводился среди сотрудников МВД по РТ, проходивших обучение по дополнительной программе повышения квалификации сотрудников следственных и экспертно-криминалистических подразделений, подразделений дознания, специально-технических мероприятий, уголовного розыска, по контролю за оборотом наркотиков, противодействию экстремизму, экономической безопасности и противодействию коррупции территориальных органов МВД России, осуществляющих функции по противодействию преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий, в образовательных организациях МВД России, расположенных по месту совместной дислокации. КЮИ МВД России, г. Казань, 2017.

терной системой или сетью, включая такие преступления, как незаконное хранение, предложение или распространение информации посредством компьютерной системы или сети.

Ко второй категории мы и относим понятие «преступления, совершаемые с использованием высоких технологий и телекоммуникаций».

Далее рассмотрим основной категориальным аппарат, используемый в законодательстве и юридической литературе применительно к преступлениям, совершаемым с использованием высоких технологий и телекоммуникаций.

Компьютерная информация - информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи[1].

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации[2].

Компьютерный взлом – несанкционированное проникновение в компьютерную сеть с целью получения собственной выгоды, например, хищения денег на счетах в банках[3].

Хищение денежных средств, совершаемое с использованием высоких технологий – это совершенное с корыстной целью противоправное безвозмездное изъятие и обращение чужих денежных средств, числящихся на банковских и иных счетах, в

---

[1] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

[2] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон РФ от 26.07.2017 № 187-ФЗ. Доступ из СПС «Консультант плюс» (дата обращения 12.08.2017).

[3] Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б. Современный экономический словарь. 6-е изд., перераб. и доп. М.: ИНФРА-М, 2011.

пользу лица, совершившего данное преступление, или других лиц путем применения средств хранения, обработки и (или) передачи компьютерной информации, причинившее ущерб их собственнику или иному владельцу. К такого рода преступлениям можно отнести кражу (ст. 158 УК), мошенничество с использованием платежных карт (ст. 159.3 УК), мошенничество в сфере компьютерной информации (ст. 159.6 УК), присвоение и растрату (ст. 160 УК).

1.2. Классификация преступлений, совершаемых с использованием высоких технологий и телекоммуникаций

Исследователи, занимающиеся проблемой киберпреступлений, предлагают различные классификации. Их подразделяют на виды в зависимости от объекта и предмета посягательства и т.д.

Конвенция о преступности в сфере компьютерной информации (ETS N 185) предлагает следующую классификацию:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

✓ противозаконный доступ (статья 2), когда он является преднамеренным, к компьютерной системе в целом или любой ее части неправомерно, если он совершен с нарушениями мер безопасности и с намерением завладеть компьютерными данными или иным умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой;

✓ неправомерный перехват (статья 3) – умышленно неправомерно осуществленный с использованием технических средств перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные,

если он был совершен с умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой;

✓ воздействие на данные (статья 4) – умышленное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных неправомерно;

✓ воздействие на функционирование системы (статья 5) – умышленное создание неправомерно серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных;

✓ противозаконное использование устройств (статья 6) – нижеследующие деяния в случае их совершения умышленно и неправомерно:

а) производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование устройств, включая компьютерные программы, разработанных или адаптированных прежде всего для целей совершения какого-либо из правонарушений, компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части;

б) владение одним из упомянутых предметов с намерением использовать его для совершения каких-либо правонарушений.[1]

2. Правонарушения, связанные с использованием компьютерных средств:

✓ подлог с использованием компьютерных технологий (статья 7) умышленный и неправомерный ввод, изменение, стирание или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качест-

[1] Конвенция о преступности в сфере компьютерной информации (ETS № 185). Доступ из СПС «Консультант плюс» (дата обращения 12.08.2017).

ве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными.

✓мошенничество с использованием компьютерных технологий (статья 8) – умышленное и неправомерное лишение другого лица его собственности путем:

а) любого ввода, изменения, удаления или блокирования компьютерных данных;

б) любого вмешательства в функционирование компьютерной системы, мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

3. Правонарушения, связанные с содержанием данных (правонарушения, связанные с детской порнографией (статья 9)):

а) производство детской порнографической продукции в целях распространения через компьютерную систему;

б) предложение или предоставление в пользование детской порнографии через компьютерную систему;

в) распространение или передача детской порнографии через компьютерную систему;

г) приобретение детской порнографии через компьютерную систему для себя или для другого лица;

д) владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.

4. Правонарушения, связанные с нарушением авторского права и смежных прав (статья 10):

Правонарушения, связанные с нарушением авторского права и смежных прав

а) нарушения авторского права, когда такие действия совершаются умышленно в коммерческом масштабе и с помощью компьютерной системы;

б) нарушения прав, связанных с авторским правом, когда такие акты совершены умышленно, в коммерческом масштабе и с помощью компьютерной системы.

Далее рассмотрим классификацию в зависимости от способа совершения преступлений с использованием высоких технологий и телекоммуникаций.

Кардинг – жаргонное название преступлений с банковскими картами – в них незаконно используются сами карты или информация о них.

Различают «кардинг-он-лайн», включающий применение скомпрометированных карт в интернет-магазинах, «кардинг-офф-лайн» – использование карт для расчета в традиционных торгово-сервисных предприятиях (ТСП) и «кэшинг» – съем денег в банкомате (АТМ) по скомпрометированным картам. Занимаясь кардингом, можно либо получить информацию о реальной карте, либо сгенерировать все эти данные. Интересующиеся могут свободно найти ссылки на сайты, которые открыто торгуют сведениями о банковских картах.

Подделка карты – изготовление карт, реквизиты которых полностью повторяют реквизиты реальных карт, выпущенных эмитентом. По поддельному «пластику» можно совершать операции, выдавая его за настоящий.

Скимминг (skimming) – незаметное для держателя реальной карты копирование данных с магнитной полосы с помощью специальных устройств на банкомате. Собираются данные клиентов банка, которые воспользовались данным банкоматом, после чего на специальную заготовку записывается дамп карты потерпевшего и снимаются деньги прямо в банкомате, т.к. скимер списывает данные с карты и записывает пин-код к ней.

Скимминговое оборудование – оборудование для несанкционированного считывания информации с банковских карт физических лиц и фиксации ПИН-кодов к ним.

Сниффинг (от англ. to sniff – нюхать) – перехват и анализ сетевого трафика с помощью сниффера (программы или устройства). Сниффер может анализировать только то, что проходит че-

рез его сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются всем машинам, из-за этого возможно перехватывать чужую информацию. Коммутация пакетов — форма передачи, при которой данные, разбитые на отдельные пакеты, могут пересылаться из исходного пункта в пункт назначения разными маршрутами. Так что если кто-то в другом сегменте посылает внутри него какие-либо пакеты, то в ваш сегмент коммутатор эти данные не отправит.

Снятие дампа карты (дамп - данные с магнитной ленты карты). Снятые данные записываются на заготовку карты, на которой принтером наносится изображение какого-либо банка и иногда эмбасируется номер карты и имя владельца, и в дальнейшем приобретаются какие-либо товарно-материальные ценности, так как не во всех терминалах нужен пин-код карты.

Фарминг — метод онлайнового мошенничества, заключающийся в изменении *DNS* (*Domain Name System*) адресов так, чтобы веб-страницы, которые посещает пользователь, были не оригинальными, а другими, специально созданными кибермошенниками для сбора конфиденциальной информации. Необходимая для инфицирования программа-вирус скрытно устанавливается на каждый компьютер бот-сети.

Фишинг (phishing – производное от phone –телефон и fishing – рыбалка) – преступление, в котором все персональные данные о картах и счетах клиента добываются злоупотреблением доверием (мошенничеством) **–** всю требуемую информацию владельцы карт передают преступникам добровольно. Часто фишинг осуществляется рассылкой по электронной почте официального письма якобы от имени представителя банка.

DDoS атаки. Бот-сети (botnets) – сети в Интернет зомбированных (инфицированных) компьютеров. Зараженный компьютер-бот в дальнейшем используется для рассылки спама, проведения «атак на отказ в обслуживании» (Distributed Denial of Service – DDoS), организации клик-фрода. Необходимая для ин-

фицирования программа-вирус скрытно устанавливается на каждый компьютер бот-сети.

Криптолокинг – блокирование доступа к данным на персональном компьютере или ином устройстве, в облачном хранилище с последующими незаконными требованиями передачи денежных средств или ином вознаграждении за его разблокировку.

Платежное мошенничество: EMV (чип и PIN-код), геоблокировка и другие промышленные меры безопасности продолжают помогать в эффективной борьбе с карточным мошенничеством, но, тем не менее, растет и число атак, направленных против банкоматов. Организованные преступные группы начинают компрометировать платежи, связанные с использованием бесконтактных карт (NFC).

1.3. Криминалистические особенности преступлений, совершаемых с использованием платежных пластиковых карт

По данным Национального агентства финансовых исследований, в 2016 г. в среднем у каждого пользователя банковской карты имеется 2,3 карты[1]. Согласно данным правоохранительных органов РФ, среди преступлений с использованием высоких технологий наибольшие темпы роста имеют показатели количества противоправных деяний с использованием платежных карт[2].

Пластиковая карта **–** обобщающий термин, который обозначает все виды карточек, различающихся по назначению, по набору оказываемых с их помощью услуг, по своим техническим возможностям и организациям, их выпускающим. Важнейшая особенность всех пластиковых карт, независимо от степени их

[1] Безопасность банковских карт: взгляд потребителя и активность игроков рынка. Отчет по результатам исследования. М.: Национальное агентство финансовых исследований, 2017.URL:http://nacfin.ru/wpcontent/uploads/2017/01/moshennichestvo_bankovskie_karty.pdf.
[2] Козловский В. Масштабы кибермошенничества растут // Российская газета. 2012. 29 ноября. URL: http://www.rg.ru/2012/11/29/karti-site.html.

совершенства, состоит в том, что на них хранится определенный набор информации, используемый в различных прикладных программах.

Под **банковской (платежной) картой** понимается средство для составления расчетных и иных документов, подлежащих оплате за счет клиента, т.е. физического или юридического лица, заключившего с кредитной организацией-эмитентом банковской карты договор, предусматривающий осуществление операций с ее использованием. Она представляет собой пластиковый прямоугольник со специальной магнитной полосой, в памяти которой хранится информация, необходимая для расчетов за товары (работы, услуги) либо для снятия наличных денег за счет имеющихся на карточном счете сумм.

Магнитная банковская карточка – это только отражение банковского счета владельца: ее магнитный индикатор содержит лишь информацию об имени владельца и номере его счета в банке. Поэтому при расчетах с использованием этой карты каждый раз необходимо обращаться к центральному компьютеру для получения информации о наличии на счете необходимой для оплаты товаров (работ, услуг) суммы денег. При использовании магнитной карты следует пройти процедуру персонификации - уточнения того факта, что картой владеет именно ее предъявитель. Связь с системным кассовым терминалом нужна для дачи команды на списание определенной суммы денег, подлежащей оплате.

Чиповая карточка содержит микропроцессор (чип) – маленький квадратик или овал на лицевой стороне, в памяти которого содержится вся информация о банковском счете ее владельца: о количестве денег на счете, максимальном размере суммы, которую можно снять со счета единовременно, об операциях, совершенных в течение дня. Чиповая карточка – это одновременно и кошелек, и средство расчета, и банковский счет. И это все благодаря микропроцессору, главным достоинством которого явля-

ется его высокая способность при постоянстве памяти надежно сохранять и использовать большие объемы информации. При этом чиповая карточка не нуждается в процедуре идентификации и персонификации, а значит, способна работать в режиме off-line, что не требует обращения при каждом необходимом случае к банку или компании, где открыт счет владельца карты.

При осуществлении платежей при помощи электронного средства платежа нет необходимости в заведении отдельного банковского счета. Перемещение электронных денежных средств происходит не по банковским информационным системам, а по специально предназначенным для этой карты сетям, где они хранятся на консолидированном счете. Электронные денежные средства представляют собой определенную информацию, которая была конвертирована в эквивалент, выраженный в стоимостной или натуральной единице (деньги, минуты, количество поездок, литры и т.д.). В зависимости от территории действия различают карты локального характера, использование которых возможно в офисах, банкоматах банка эмитента, как правило, в пределах одной страны (Оперативная российская платежная система Сберкарт), и международного характера, используемые в качестве универсального средства платежа на территории стран-участников, где принимаются данные карты (Visa, Master Card, Diners Club, American Express, JCB и China Unionpay).

Каждая карта подлежит процедуре персонализации, в соответствии с которой ей присваивается определенный номер, имя держателя, срок действия. При этом все необходимые данные, связанные с информацией о держателе карты, наносятся на магнитную полосу и (или) в память микропроцессора карты, при наличии чипа. При совершении каких-либо операций с картой денежные средства могут поступать как с одного счета, к которому привязана карта (кредитная или расчетная), так и с нескольких счетов клиента, к которым эта карта также привязана. Для удобства клиента допускается также использование нескольких карт

по одному счету, например, для членов семьи. Для юридических лиц и индивидуальных предпринимателей предусматриваются определенные ограничения на снятие наличных денежных средств в течение одного операционного дня. Для физических лиц банки и иные кредитные организации устанавливают собственные денежные лимиты.

Организованные преступные группы кардеров нередко совершают несколько эпизодов мошенничества. Так, в городе Ухте были задержаны участники преступной группы, состоящей из трех человек, занимавшихся мошенничеством с использованием поддельных платежных карт (23 эпизода хищений). Члены организованной преступной группы по фальшивой банковской карте приобрели на одной АЗС 900 л бензина на 22140 руб., а на другой – 3658 л дизельного топлива на 100960 руб. Эмитентами пластиковых карт, которые были задействованы при совершении преступления, являлись банки США, Испании, Франции и Швейцарии. Для совершения мошенничества преступники использовали специальное оборудование по изготовлению поддельных пластиковых карт[1].

Специалисты отмечают, что, как и другие киберспреступления, преступления с использованием платежных карт нередко совершаются членами разветвленных, хорошо организованных преступных групп, участники которых имеют свою преступную специализацию[2]. Криминальная специализация в группе может выглядеть следующим образом: одни члены группы осуществляют сбор информации по платежным картам, другие – обрабатывают собранную информацию и передают их тем, кто занимается изготовлением поддельных карт. Подготовленное таким образом хищение осуществляют лица, специализирующиеся на «вещевом» кардинге – именно они используют платежную карту для обмана

[1] Попова Н. Российские банкоматы оказались в ливанской петле // АН-online. URL: http://argumenti.ru/crime/2012/02/156477, свободный.

[2] Козловский В. Масштабы кибермошенничества растут // Российская газета. 2012. 29 ноября. URL: http://www.rg.ru/2012/11/29/karti-site.html, свободный.

работников торговой организации.

Еще одним основанием для классификации способов мошенничества с использованием платежных карт является технологическое решение, задействованное преступниками при совершении преступления. В статье 159.3 УК РФ указаны два способа совершения такого мошенничества: с использованием поддельной (1) или принадлежащей другому лицу (2) платежной карты. Примером последнего является дело, в ходе расследования которого было установлено, что К., совершив тайное хищение имущества, завладел платежной картой потерпевшего и решил использовать ее для осуществления мошенничества. С целью реализации своего умысла К. неоднократно использовал похищенную платежную карту для приобретения различных товаров[1].

Сегодня до 80 % обращений через интернет-сайт МВД РФ посвящены мошенничеству при покупке товаров через социальные сети и интернет-магазины. Также продолжает расти разнообразие вредоносных программ для мобильных устройств.

Целью злоумышленников может быть получение доступа к мобильному банку жертвы и к конфиденциальным сведениям.

В 2016 г. зафиксировано увеличение числа программ, используемых для реализации мошеннических схем. Они имеют широкий функционал – от получения данных банковских карт до снятия наличных денег и несанкционированного проникновения во внутреннюю сеть банка. Не теряет популярность и «классический» скимминг. Обобщенные данные в области разработки безопасных приложений и оценки уязвимостей показывают следующую статистику:

1. В 2016 году злоумышленник оказался способен получить доступ к узлам внутренней сети субъекта национальной платежной системы в 9 случаях из 10, а в 2012 году аналогичное соотношение составляло 7 из 10;

[1] Приговор Верхнепышминского городского суда от 7 июня 2011 г. по уголовному делу № 1-152/11. URL. http://docs.pravo.ru/document/view/18392970/.

2. Для проведения атаки в 82 % случаев достаточно иметь среднюю или низкую квалификацию;

3. Факторы уязвимости web-приложений обнаружены в 93 % исследованных систем;

4. Причинами возникновения уязвимостей в АБС являются ошибки (недостатки) разработки (23 %) и отсутствие эффективных защитных механизмов (43 %);

5. Уязвимости приложений – один из распространенных факторов, способствующих проникновению в корпоративные сети[1].

Рассмотрим основные приемы мошеннических действий, следующие из российской специфики. Самый распространенный способ – халатность и правовой нигилизм клиентов, которые разглашают PIN-код путем его записи на карту или путем так называемого «дружественного мошенничества» – разглашения PIN-кода членам семьи, близким друзьям, коллегам.

Еще пример – когда из-за фактора технической неграмотности клиенты впадают в панику при получении SMS-сообщения «Ваша банковская карта заблокирована» со всеми вытекающими для них последствиями.

Хищения денежных средств в системе ДБО или путем несанкционированного входа в компьютерную систему кредитных организаций либо использования сбоев в ее работе связаны с операциями с компьютеров жертв и основаны на функциональных возможностях автоматической подмены платежных распоряжений в момент их отправки пользователями, а также автоматизированных процессах формирования и отправки платежного поручения.

Как правило, несанкционированный доступ на компьютерное устройство жертвы осуществляется путем его заражения вредоносными программами через уязвимости системного и прикладного программного обеспечения (операционные системы, WEB-браузеры, почтовые клиенты, социальные сети и т.д.) с по-

[1] Выборнов А. Устранение уязвимостей // BIS journal. 2014. № 4.

следующим дистанционным похищением паролей и использованием ключей электронной подписи. Так, 27 февраля 2015 г. с 12.30 ч. до 13.00 ч. путем неправомерного доступа к компьютерной информации, хранящейся на жестком диске персонального компьютера директора (начальника) казначейства АКБ «Энергобанк» (ОАО), в котором установлено второе рабочее место участника торгов на Московской межбанковской валютной бирже «Национальный клиринговый центр» (ММВБ), совершена модификация компьютерной информации, позволившая осуществить сделки с валютными денежными средствами в сумме более 4 000 000 000 рублей путем покупки 158 737 000 долларов США по среднему курсу 62, 62 рубля за 1 доллар США и продажи 93 925 000 долларов США по среднему курсу 59, 67 рублей за 1 доллар США через Московскую межбанковскую валютную биржу «Национальный клиринговый центр», причинившая ущерб АКБ «Энергобанк» (ОАО) на общую сумму 469 861 520 рублей[1].

1.4. Криминологическая характеристика преступлений, совершаемых с использованием высоких технологий и телекоммуникаций

Обстановка совершения преступлений с использованием высоких технологий и телекоммуникаций характеризуется рядом существенных факторов. Для нее характерно несовпадение между местом совершения противоправных действий и местом наступления общественно опасных последствий.

Субъекты данных преступлений нередко владеют специальными навыками не только в области управления компьютера и устройствами, но и специальными знаниями в области обработки информации в информационных системах в целом. При этом для корыстных преступлений, связанных с использованием инфор-

[1] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий. М., 2016. С. 63 - 69.

мационных систем, характерны и специальные познания в соответствующих финансовых и иных информационных технологиях.

Субъекты могут различаться как по уровню их профессиональной подготовки, так и по социальному положению.

Специалисты подразделяют лиц и организации, осуществляющие атаки, на несколько категорий. Однако между этими категориями не существует достаточно четких границ. Таким образом, деление на группы можно считать в каком-то смысле условным[1].

Рассмотрим наиболее распространенные профили лиц, совершающих преступления с использованием высоких технологий и коммуникаций.

Дропы - играют важную роль в киберпреступлениях, именно они превращают похищенные логины и PIN-коды в реальные деньги. Работа дропа наиболее опасна - дроп снимает деньги в банкомате и затем передает их заказчику.

Кодеры - квалифицированные программисты, изготавливающие преступные инструменты - программы-вирусы, пользовательские боты, программы для рассылки спама и др. Часто кодеры предлагают сами преступные услуги. Поставляя программы, кодер минимизирует риск быть наказанным.

Кракеры (*crackers*) — специалисты, способные снять защиту от копирования с лицензионного программного обеспечения.

Хакеры – лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций.

Хактивисты – используется для обозначения явления социального протеста, которое представляет собой своеобразный синтез социальной активности, преследующей цель протеста против чего-либо, и хакерства (использования интернет-технологий с целью причинения ущерба компьютерным сетям и их пользователям).

[1] Яблоков Н.П. Криминалистика: учебник. М.: ЛексЭст, 2006.

Инсайдер – лицо, имеющее в силу своего служебного или семейного положения доступ к конфиденциальной информации о делах компании. В эту группу включаются лица, добывающие конфиденциальную информацию о деятельности корпорации и использующие ее в целях личного обогащения.

Провайдеры, обслуживающие мошенников – в Интернете организованы AntiAbuseHosting сети («абузоустойчивые» хостинги - на сленге), позволяющие размещать любые противоправные сайты и при этом защищать владельцев этих сайтов от действий правоохранительных органов. В целях «шифровки» своих клиентов недобросовестные провайдеры используют промежуточные прокси-серверы и VPN-серверы – это позволяет удлинить цепочку, ведущую к преступникам.

Шпионы – лица, взламывающие компьютеры для получения информации, которую можно использовать в политических, военных и экономических целях.

Террористы – лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать в целях политического воздействия.

Вандалы – лица, взламывающие информационные системы для их разрушения.

Психически больные лица, страдающие новым видом психических заболеваний – информационными болезнями или компьютерными фобиями.

Зарубежный учёный М. Роджерс выделил следующие группы преступников в зависимости от уровня их технической подготовленности:

- ✓ новички (tool kit newbie, script kiddies);
- ✓ кибер-панки (cyber-punks);
- ✓ свои – служащие организации-жертвы (internals);
- ✓ кодировщики (coders);
- ✓ хакеры «старой гвардии» (old guard hackers);
- ✓ профессиональные преступники (professional criminals);
- ✓ кибертеррористы (cyber-terrorists).

Глава 2.
ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНЫХ ДЕЛ, ТАКТИКА ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ И ТЕЛЕКОММУНИКАЦИЙ

2.1. Возбуждение уголовных дел и планирование расследования преступлений, совершаемых с использованием высоких технологий и телекоммуникаций. Типичные следственные ситуации и версии

Обращению в ОВД с заявлением о преступлении, как правило, предшествуют попытки пострадавшего или его представителя установить причины уменьшения денежных средств на счете, связанные с внутренней проверкой организации факта списания с ее банковского счета денежных средств, в том числе с уведомлением и содействием в проверке коммерческого банка или иной платежной системы.

Такой временной интервал между событием преступления и обращением в ОВД дает преступникам достаточно времени для сокрытия следов хищений.

Несмотря на длительность времени, прошедшего с момента обнаружения хищения до обращения пострадавших с заявлением о преступлении, органы дознания или следователи должны организовать и провести комплекс мероприятий, включая фиксацию

следов преступления на электронных носителях информации, отслеживание соединений с компьютерным устройством и иные[1].

Проведенные Н.В. Олиндер и А.Н. Яковлевым исследования показали, что типичными поводами для возбуждения уголовных дел о преступлениях, совершаемых с использованием высоких технологий и телекоммуникаций, являются:

1. Заявление о преступлении, поступившее от потерпевшего – представителя юридического лица или от гражданина – физического лица (63 %). Правообладатель или собственник информационной системы выявил нарушения конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Непосредственное обнаружение признаков преступления органом дознания (20 %):

✓ в результате проверки сообщения о совершенном или готовящемся преступлении, поступившего из оперативных источников;

✓ в ходе проведения специальных оперативно-технических мероприятий;

✓ по результатам анализа материалов контрольно-ревизионных и иных документальных проверок;

✓ при задержании лица (лиц) на месте совершения преступления с поличным.

3. Непосредственное обнаружение признаков преступления следователем или прокурором при расследовании уголовных дел о преступлениях других видов (9 %).

4. Сообщения в средствах массовой информации и иные поводы (8 %).[2]

[1] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Указ. соч. С. 97 - 98.

[2] Яковлев А.Н., Олиндер Н.В. Особенности расследования преступлений, совершаемых с использованием электронных платежных средств и систем: методическое пособие. М., 2012. С. 62 - 63.

На основе анализа уголовных дел, связанных с преступлениями, совершенными с использованием высоких технологий, можно предложить некоторую обобщенную схему расследования подобных преступлений.

В ходе расследования основные следственные задачи целесообразно решать в такой последовательности:

1. Установление факта неправомерного доступа к информации в компьютерной системе или сети.
2. Установление места несанкционированного проникновения в компьютерную систему или сеть.
3. Установление времени совершения преступления.
4. Установление способа несанкционированного доступа.
5. Установление лиц, совершивших неправомерный доступ, их виновности и мотивов преступления.
6. Установление вредных последствий преступления.
7. Выявление обстоятельств, способствовавших преступлению, и в том числе установление надежности средств защиты компьютерной информации.

При расследовании компьютерных преступлений, связанных с созданием, использованием и распространением вредоносных программ для ПК, целесообразно применять следующую последовательность действий:

1. Установление факта использования и распространения вредоносной программы.
2. Установление факта и способа создания вредоносной программы.
3. Установление лиц, виновных в создании, использовании и распространении вредоносных программ.
4. Установление вреда, причиненного данным преступлением.
5. Установление обстоятельств, способствовавших совершению расследуемого преступления.

К типичным признакам подготовки, совершения и сокрытия преступления в сфере компьютерной информации относятся:

- появление в системе ПК или их сети ложных данных (письма электронной почты от неизвестных и известных адресатов с прикрепленными файлами, не соответствующими описанию и т.п.);

- несанкционированные изменения программного обеспечения и конфигурации ПК, системы ПК или их сети;

- частые сбои в работе аппаратуры;

- жалобы клиентов на предоставление некачественного доступа к ПК, системе ПК, их сети или компьютерной информации;

- нерегламентированный доступ к ПК, системе ПК, их сети и к компьютерной информации отдельных субъектов;

- нарушение правил работы с компьютерной информацией и несанкционированные манипуляции с ней;

- чрезмерный интерес отдельных субъектов (клиентов, сотрудников) к содержанию компьютерной информации определенной категории;

- применение на рабочем месте и вынос с работы личных носителей информации под различными предлогами;

- случаи утечки конфиденциальной информации либо обнаружение негласных устройств ее получения; нарушение установленных правил оформления документов при работе с ПК, системой ПК, их сетью или компьютерной информацией;

- создание копий определенной категории данных и компьютерной информации, не предусмотренных технологическим процессом;

- несоответствие данных, содержащихся в первичных (исходных) документах, иным более поздним по времени создания документам;

- подозрительно частое обращение одного и того же пользователя к данным и компьютерной информации определенной категории;

- появление в компьютере недостоверных данных;

- не обновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств.

С учетом комплекса исходной информации, полученной при проведении проверочных действий, на первоначальном этапе расследования могут складываться следующие типичные следственные ситуации:

1. Установлен неправомерный доступ к компьютерной информации, есть следы, есть подозреваемый, который дает правдивые показания.

2. Установлен неправомерный доступ к компьютерной информации, имеются следы, прямо указывающие на конкретного подозреваемого, но он отрицает свою причастность к совершению преступления.

3. Установлен неправомерный доступ к компьютерной информации, известны лица, совершившие преступление, но обстоятельства доступа не установлены.

4. Установлен факт неправомерного доступа к компьютерной информации, совершить который и воспользоваться его результатами могли только лица из определенного круга (по своему положению, профессиональным навыкам и знаниям), либо известны лица (фирмы, организации), заинтересованные в получении данной информации.

Последняя из приведенных следственных ситуаций является наиболее сложной, так как отсутствуют сведения о виновном лице, следы преступления, неизвестен способ совершения преступления и др.

На основании вышеуказанных типичных следственных ситуаций на первоначальном этапе расследования преступлений рассматриваемого вида можно выделить следующие общие версии:

1. Состав преступления отсутствует, поскольку происшедшее событие является следствием непреодолимых факторов (самопроизвольный сбой в работе программных или аппаратных со-

ставляющих средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, сетей электропитания и связи, средств защиты информации; выход из строя машинного носителя информации по причине естественного износа и старения; саморазрушение отдельных электронных компонентов компьютерных устройств и др.).

2. Совершено неумышленное преступление по причине халатности лица, ответственного за соблюдение режима конфиденциальности соответствующей компьютерной информации.

3. Преступление совершено с целью наживы лицом, имеющим доступ к конфиденциальной информации в силу исполнения им своих служебных обязанностей, – сотрудником потерпевшего.

4. Преступление совершено лицом, знакомым с условиями обработки и защиты конкретной конфиденциальной компьютерной информации потерпевшим.

5. Преступление совершено дистанционно с использованием специальных технических средств, предназначенных (приспособленных, разработанных, запрограммированных) для негласного получения конфиденциальной информации.

Приведенный перечень следственных версий является общим и в зависимости от конкретной ситуации может быть расширен.

При выдвижении версий совершения преступлений, совершенных с использованием высоких технологий и телекоммуникаций, необходимо учитывать, что они совершаются обычно группой из двух и более человек, хотя не исключена возможность работы преступника – одиночки.

Преступление обычно происходит в рабочее время и внешне не отличается от обычной работы в учреждении. Похищенная информация используется в дальнейшем самими преступниками для подготовки хищений или может быть продана заинтересованным лицам.

В случае возбуждения уголовного дела, исходя из содержания уже имеющихся в материалах проверки документов, осуществляется планирование расследования на первоначальном этапе. Поскольку проверка сообщений о любом преступлении проводится в сроки, жестко регламентированные действующим уголовно-процессуальным законом (ч. 1 и 3 ст. 144 УПК РФ), целесообразно составить план ее проведения, в который включить: 1) организацию мероприятия по ознакомлению с сообщением и исходной информацией о преступлении, содержащейся в представленных потерпевшим материалах; 2) выдвижение версий, определение вопросов, подлежащих выяснению; 3) определение круга следственных действий и организационных мероприятий, подлежащих проведению по каждой версии, сроков и последовательности их проведения, а также исполнителей.

В план проверки заявления о преступлении рекомендуется включать следующие действия (операции):

1) получение письменного объяснения у потерпевшего (его представителя);

2) осмотр места происшествия (точка размещения банкомата, помещение с компьютером, подключенным к системе ДБО и т.п.);

3) истребование в ходе осмотра места происшествия или путем направления запроса пострадавшему документов и сведений, относящихся к событию хищения. Ознакомление с перечисленными и иными документами и осуществление их анализа;

4) получение письменных объяснений;

5) истребование в кредитных организациях сведений и документов, относящихся к хищению. Ознакомление и анализ изъятых в кредитных организациях отправителя (потерпевшего) сведений и документов;

6) истребование у интернет-провайдера или оператора связи соответствующих документов и сведений;

7) получение объяснения от работника интернет-провайдера или оператора связи (при необходимости);

8) анализ результатов осмотра места происшествия, полученных объяснений, документов и сведений для решения вопроса о необходимости производства исследований либо назначения и производства СКЭ и других судебных экспертиз;

9) дача поручений органам, осуществляющим оперативно-розыскные мероприятия (далее – ОРМ);

10) установление приемов и определение допустимости использования в уголовном деле материалов, полученных в результате осуществления оперативно-розыскной деятельности[1].

В плане могут быть предусмотрены и другие проверочные и ознакомительные действия. В очередность перечисленных следственных действий, оперативно-розыскных, проверочных и организационных мероприятий могут быть внесены коррективы[2].

2.2. Тактика производства отдельных следственных действий по уголовным делам о преступлениях, совершенных в сфере высоких технологий и компьютерной информации

При расследовании преступлений, совершаемых с использованием высоких технологий и коммуникаций, чаще всего проводятся такие следственные действия, как осмотр места происшествия, допрос, обыск, выемка и назначение судебных экспертиз.

1. Осмотр места происшествия

Осмотр – самостоятельное следственное действие, заключающееся в обследовании следователем или иным полномочным лицом объектов, виды которых названы в законе, в установленном уголовно-процессуальным законом порядке для достижения определенных целей и специфических задач.

---

[1] Лузгин И.И. Технико-криминалистическое обеспечение как мегаинструментальная технология формирования единого криминалистического пространства // Эксперт-криминалист. 2010. № 1. С. 30 - 34.

[2] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Указ. соч. С. 100 - 101.

Особое значение осмотра места происшествия как первого следственного действия, проводимого, как правило, до возбуждения уголовного дела, заключается в том, что это самое близкое во времени и в пространстве соприкосновение следователя с событием преступления[1].

Под местом происшествия по делам о преступлениях, совершаемых с использованием высоких технологий, следует понимать не только территорию или помещение, где осуществлялось противоправное действие (бездействие) либо наступили вредные последствия содеянного, но и место, где обнаружены связанные с ним обстоятельства (вредные последствия).

Местом происшествия может быть как одно помещение, где установлен компьютер и хранится информация, так и ряд помещений, в т.ч. в разных зданиях, соединенных компьютерной сетью или находящихся на различных территориях, связанных сетью Интернет. Очевидно, что в последнем случае осмотр каждого из указанных мест должен оформляться самостоятельным протоколом осмотра места происшествия.

Осмотр места происшествия должен начинаться с тщательной подготовки, заключающейся в уточнении его границ, выборе необходимых специалистов, технических средств и четком определении его объектов. Целесообразно обратиться к помощи службы безопасности той организации, в которой обнаружено правонарушение[2].

При производстве следственного действия целесообразнее всего использовать тактический прием «от центра к периферии», где в качестве «центра» (отправной точки осмотра места происшествия) будет выступать конкретное СКТ и (или) компьютерная информация, обладающая вышеуказанными свойствами. Деталь-

---

1 Васильев А.Н. Тактика отдельных следственных действий. М., 1981. С. 35.

[2] Согласно Федеральному закону «Об информации, информационных технологиях и защите информации» организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, должны создавать специальные службы, обеспечивающие ее защиту.

ное описание данных предметов, их соединений (физических и логических) должно сопровождаться видеосъемкой, фиксирующей последовательность действий следователя и специалистов, а также полученный при этом результат.

К участию в производстве осмотра места происшествия (ОМП) рекомендуется привлекать:

✓ специалиста по профилю сетевого средства вычислительной техники (ССВТ), которое нужно будет осмотреть в ходе следственного действия;

✓ специалиста, обладающего минимально необходимыми знаниями по тем операциям технологического процесса, при проведении которых были обнаружены признаки преступления;

✓ представителя администрации предприятия, учреждения или организации, на территории (в помещении) которых производится осмотр;

✓ лицо, несущее материальную ответственность за компьютерную информацию, подвергшуюся преступному воздействию, электронный носитель информации и СКТ;

✓ инспектора или ревизора, проводившего инвентаризацию, ревизию, аудиторскую или иную документальную проверку, вскрывшую признаки правонарушения.

В качестве понятых рекомендуется привлекать лиц, обладающих необходимыми специальными знаниями в области обработки компьютерной информации (на уровне бытовых пользователей компьютерной техники).

На месте происшествия по делам о преступлениях в сфере компьютерной информации рекомендуется принимать следующие меры по сохранности обстановки и фиксации значимых обстоятельств:

1. Правильное количественное определение объектов осмотра компьютерных средств в качестве вещественных доказательств.

2. Использование специально разработанного компьютерного оборудования и пакета служебного программного обеспечения.

3. Отражение в процессе осмотра не только количества выявленных компьютерных средств, но и описание их технических характеристик и состояния работоспособности.

4. Подробное описание графического интерфейса загруженной операционной системы данного компьютера с перечислением ярлыков установленных программ, что затруднит возможность их сокрытия или подмены после осмотра.

5. Закрепление виртуальных следов: более подробное описание файловой системы, прикладных программ, физических носителей информационных следов как электронных, так и бумажных с указанием места их обнаружения. Описание использованных при этом специальных программно-технических средств.

6. Фиксация последовательности проведения поисковых действий. Такое закрепление способствует более полному проведению следственного действия – «проверка показаний на месте»» (ст. 194 УПК РФ)[1].

Особенно тщательно должны быть осмотрены и описаны в протоколе типичные вещественные доказательства: вредоносное программное обеспечение и носители, на которых оно хранится; программное обеспечение, заведомо приводящие к несанкционированным пользователем действиям (влияющие на конечные результаты технологического процесса), а также их носители; обнаруженные специальные технические средства негласного получения (уничтожения, блокирования) компьютерной информации и носителей; специфические следы преступника и преступления.

Для осмотра информации можно применить специальное компьютерное оборудование и программное обеспечение, имеющееся в распоряжении следственной группы, но исследовать информацию в компьютерах на месте происшествия с помощью программного обеспечения, установленного на самих осматриваемых компьютерах, крайне нежелательно из-за опасности иска-

[1] Осмотр места происшествия: практическое пособие / под ред. А.И. Дворкина. М.: Юристъ, 2001.

зить или повредить данные. В современных компьютерах такой «осмотр» неизбежно сопровождается изменением информации на компьютерных носителях по сравнению с исходной[1].

При осмотре работающего ПК:

✓ расположение рабочих механизмов ПК и изображение на его экране (мониторе) или визуально-контрольном окне (для принтеров, контрольно-кассовых машин, контрольно-пропускных механизмов, цифровых аппаратов связи и т.д.);

✓ все действия, производимые специалистом при осмотре ПК (порядок нажатия на клавиши и запорные механизмы, корректного приостановления работы и закрытия исполняемой операции или программы, выключения ПК, отключения от источника электропитания, рассоединения или соединения ПК и его составляющих, отсоединения коммуникационных и электропитающих проводов и кабелей, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т.п.);

✓ установить, какая программа выполняется (для чего осмотреть изображение на экране дисплея и детально описать его, по возможности произвести фотографирование или видеозапись); тип программного обеспечения, загруженного в момент осмотра в компьютер, может свидетельствовать о задачах, для которых использовался данный компьютер;

✓ по мере необходимости и возможности остановить исполнение программы и установить, какая информация получена после окончания ее работы;

✓ установить наличие в компьютере накопителей информации (жесткие диски, дисководы для дискет, стримеры, оптические диски, флэш-карты и т. п.), их тип (вид) и количество;

✓при наличии технической возможности скопировать информацию, которая может иметь значение для дела (программы, файлы данных), и имеющуюся в компьютере (особенно это важ-

[1] Пропастин С.В. Следственный осмотр: проблема определения целей и задач // Современное право. 2012. № 5. С. 133 - 135.

но для информации, находящейся в оперативном запоминающем устройстве, поскольку после выключения компьютера она может быть уничтожена).

Целесообразно исследовать компьютер на наличие удаленных файлов. Некоторые операционные системы при недостаточности объема оперативной памяти создают так называемый «файл подкачки» (файл с расширением «swp») для хранения всей удаленной информации, которая при наличии специальной программы может быть восстановлена.

Рекомендуется также изучать не только подлинники изъятых машинных носителей, но и их копии, изготовленные средствами данной операционной системы. Следует обращать внимание и на поиск так называемых «скрытых» файлов (как правило, системных защищенных от записи файлов).

Отметим, что, во избежание уничтожения (повреждения) ПК и характерных следов преступления, при работе специалиста по осмотру ПК недопустимо использование магнитосодержащих материалов, инструментов, приборов и оборудования, направленных источников электромагнитного излучения.

Следователям не рекомендуется самостоятельно, без участия специалиста, выключать работающий в момент осмотра компьютер, поскольку это может создать сложности при повторном входе в систему, особенно защищенную.

Осмотр машинного носителя начинается с определения типа, вида, назначения, технических параметров и ознакомления с его содержанием.

В процессе осмотра места происшествия (или машинного носителя информации) необходимо указать в протоколе:

- ✓ место обнаружения носителя информации;
- ✓ наличие, индивидуальные признаки и техническое состояние футляра (коробки, упаковки, специального технического устройства);
- ✓ тип, вид, марку, назначение, цвет и заводской номер;

✓ техническое состояние – размеры носителя, внешний вид, материал каркаса носителя, его целостность и индивидуальные признаки, материал основного информационно-несущего слоя и его целостность;

✓ работоспособность и внутреннюю спецификацию - серийный номер и (или) метка тома либо код; размер разметки, размер области носителя, свободной от записи и занятой под информацию; количество и номера сбойных зон, секторов, участков, кластеров; количество записанных программ, файлов, каталогов (подкаталогов), данных, их структура, название (имя и/или расширение), размер и объем, который занимают их названия, дата и время создания (или последнего изменения), а также специальная метка или флаг (системный, архивный, скрытый, только для чтения или записи и т. д.); наличие скрытых или ранее стертых файлов (программ) и их реквизиты (название, размер, дата и время создания или уничтожения);

✓ результат осмотра содержимого файлов (программ, компьютерной информации);

✓ все манипуляции (нажатия на клавиши и т. д.) со средствами вычислительной техники, совершенные в процессе осмотра.

При изъятии магнитного носителя машинной информации нужно помнить, что он должен перемещаться в пространстве и храниться исключительно в специальном экранированном контейнере или алюминиевом футляре (оболочке). Для этого магнитные носители информации сначала упаковывают в пакет из обычной фольги (бытового или технического назначения), а затем опечатывают обычным способом, вкладывая в коробку или конверт.

Недопустимо приклеивать что-либо непосредственно на магнитный носитель информации и документы, пропускать через них бечеву, пробивать степлером, делать пометки или маркировки, накалывать твердым предметом знаки, использовать пластилиновые или сургучовые печати и т. д.

Недопустимо производить изъятие в несколько приемов, в том случае, если следователь не располагает необходимым транспортом, следует сделать несколько рейсов от объекта до места хранения изъятых материалов с выставлением охраны на объекте изъятия (охране подлежат неизъятые ПК и помещение, в котором они находятся).

Стоит обратить особое внимание на то, что перед началом производства любых следственных действий, непосредственно связанных с ПК, средствами и системами их защиты, необходимо в обязательном порядке получать и анализировать с участием специалистов информацию о технологических особенностях функционирования вышеприведенных технических устройств, уровня их соподчиненности и используемых средств связи и телекоммуникации во избежание их разрушения, нарушения заданного технологического ритма и режима функционирования, причинения крупного материального ущерба пользователям и собственникам, уничтожения доказательств.

2. *Осмотр средств мобильной связи и иных мобильных устройств*

Практически при каждом расследовании преступлений, совершаемых с использованием высоких технологий и телекоммуникаций, имеется необходимость провести осмотр обнаруженного и (или) изъятого средства

сотовой связи (мольного устройства), который, как правило, делится на несколько этапов:

- ✓ внешний осмотр, в ходе которого происходит непосредственное изучение и фиксация наружного строения и состояния мобильного устройства, в рамках которого в протоколе указываются марка, модель, тип, форма аппарата, цвет корпуса, размер; наличие объективов тыльной и (или) лицевой фото/видеокамеры (вспышки), фирменных наименований, логотипа, обозначений; количество и расположение функциональных, встроенных, сенсорных клавиш (джойстика); разъемов

Mini(Micro)USB, зарядного устройства, стереонаушников; наличие отверстий для динамика, микрофона, датчика расстояния, внешней освещенности. Отдельно указываются особые приметы наружного строения: повреждения - сколы, царапины, потертости, отсутствие должных элементов; наличие дополнительных атрибутов и технических составляющих - чехла, шнурка, брелока, гарнитуры, полимерных наклеек, графических вставок, надписей, инкрустации драгоценными металлами и др. В ходе внешнего осмотра проводится детальная фотосъемка внешней, оборотной, боковых панелей мобильного устройства. В случае, если осматриваемый телефон раскладного («бабочка») или раздвижного типа («слайдер»), то телефон фотографируется в первоначальном и раскладном/раздвижном состоянии;

- ✓ конструктивный осмотр - осмотр конструкции телефона по частям - задней крышки телефона и (или) аккумуляторной батареи (в определенных моделях аппаратов сотовой связи батарея встроена в корпус либо в заднюю крышку), флеш-карты, SIM-карт(ы). При осмотре аккумуляторной батареи в протоколе следует указать ее идентификационный номер, тип, марку, модель, мощность, иную информацию, указанную на корпусе. Также в протоколе указывается цвет и родовой материал, из которого изготовлена батарея. При осмотре флеш-карты (MiniSD) необходимо обратить внимание на ее идентификационный номер, объем, цвет и родовой материал корпуса. SIM- карта, обнаруженная в телефоне, осматривается аналогичным образом. Как правило, на корпусе SIM-карты имеется логотип оператора сотовой связи, описание которого также обязательно в протоколе. В ходе конструктивного осмотра проводится детальная фотосъемка внешней и оборотной стороны батареи, флеш-карты, SIM-карты, а также тыльной стороны корпуса мобильного телефона (без задней крышки) так, чтобы на снимке был виден IMEI-номер мобильного устройства;

✓ осмотр информационной среды, включающий изучение и фиксацию сведений, которые содержатся в памяти телефона, флеш-карты, SIM-карты. В случае если в ходе осмотра следователю удалось включить мобильный телефон, и получен доступ к сведениям, которые в нем находятся, в протоколе в хронологическом порядке фиксируются все производимые в дальнейшем с устройством манипуляции[1].

В ходе осмотра мобильных устройств, смартфонов и планшетных компьютеров крайне рекомендуется использование специализированного программного обеспечения и (или) программно-аппаратных комплексов. Таких комплексов в настоящее время существует три - это UFED (производства фирмы Cellebrite, Израиль) и XRY (производства компании Micro Systemation, Швеция), «Мобильный криминалист».

В соответствии с приказом председателя следственного комитета РФ в 2012 – 2013 годах все следственные управления следственного комитета РФ были обеспечены аппаратно-программными комплексами UFED. Исходя из спецификации данного оборудования, UFED представляет собой средство для проведения оперативного исследования мобильных устройств. Аппаратно-программный комплекс позволяет провести упрощенное и быстрое логическое извлечение информации из обширного ряда мобильных устройств: мобильных телефонов, смартфонов, планшетов, телефонов китайской сборки на базе микропроцессора, некоторых моделей GPS-приемников, сим-карт мобильных устройств и карт памяти.

Второй упомянутый нами программно-аппаратный комплекс, XRY, появился на рынке раньше UFED, и на сегодня его активно используют в правоохранительной системе Великобритании и США.

[1] Шмонин А.В. Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Указ. соч. С. 155-156.

Комплекс работает в трех режимах, сходных с режимами UFED: XRY Logical (для быстрого извлечения активных данных), XRY Physical (для физического извлечения (дампа) памяти мобильного устройства), XRY Complete (полнофункциональное решение, объединяющее все инструменты и преимущества логического и физического извлечения данных).

Аналогично с комплексом UFED в результате исследования телефонов создаются защищенные от несанкционированного доступа отчеты, которые можно вывести на печать или записать на носитель.

Комплекс XRY позволяет извлекать данные из многочисленных программных приложений смартфонов. С его помощью можно извлечь данные вызовов IP-телефонии, картографическую информацию GPS и журналы средств оперативной пересылки сообщений.

Программный комплекс «мобильный криминалист» по своим характеристикам схож с упомянутыми выше техническими решениями. Его преимущество в относительном доступности продукта.

Необходимо также отметить, что есть и новые технологии, позволяющие обойти защиту мобильного телефона и, как следствие, провести осмотр с максимальной степенью эффективности. Так, обойти защиту iPhone (начиная с версии 4) исключительно программными методами практически невозможно без риска повреждения данных, но устройство IP Box iPhone Password Unlock Tool (Китай), которое появилось в открытой продаже во втором квартале 2015 года, позволяет подключиться в iPhone или iPad и методом брутфорса (перебора) подобрать запрашиваемый при загрузке операционной системы iOS пароль[1].

[1] Яковлев А.Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: "электронная почта" // Вестник Воронежского института МВД России. 2014. № 4. С. 46.

3. Допрос

Особенности тактики допроса участников уголовного дела о преступлении, совершенном с использованием высоких технологий, зависят от процессуального статуса допрашиваемого лица и ситуации производства следственного действия. Принимая решение о допросе конкретного лица в качестве свидетеля, следователь должен заранее прогнозировать, какую информацию (прежде всего технического характера) он может получить от допрашиваемого. Ориентируясь на это, необходимо заранее продумывать комплекс постановочных вопросов.

В процессе допроса свидетелей всякий раз необходимо выяснить:

✓ не было ли сбоев в работе программ, хищений носителей информации и отдельных компьютерных устройств;

✓ зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств зашиты компьютерной информации;

✓ зафиксированы ли в последнее время случаи срабатывания средств защиты компьютерной информации (антивирусные программы);

✓ как часто проверяются программы на наличие вирусов, каковы результаты последних проверок;

✓ как часто обновляется программное обеспечение, каким путем оно приобретается;

✓ каким путем приобретается компьютерная техника, как осуществляется ее ремонт и модернизация;

✓ как осуществляется защита компьютерной информации, каковы применяемые средства и методы защиты и др.

В процессе допроса системных администраторов и специалистов по информационной безопасности выясняется:

✓ перечень используемого программного обеспечения и его классификация (лицензионное, собственное);

✓ пароли защиты программ, отдельных устройств компьютера, частота их смен;

- ✓ технические характеристики компьютерной сети (при ее наличии), кто является администратором сети;
- ✓ порядок приобретения и сопровождения программного обеспечения;
- ✓ существование идентификационных программ, наличие в рабочих программах специальных файлов протоколов, регистрирующих вхождение в компьютер пользователей, каково их содержание и др.

По делам рассматриваемой категории допрос специалиста, эксперта имеет следующие особенности.

Допрос специалиста может производиться для разъяснения следователю вопросов, связанных с техническими, организационными, правовыми аспектами компьютерных технологий, используемых при совершении хищения; особенностей функционирования локальной сети; особенностей подключения к сети Интернет; иных вопросов. Особенность таких допросов в том, что специалист не только дает пояснения следователю по поставленным вопросам, но и выполняет как бы «перевод» сказанного иными участниками судопроизводства (обвиняемым, подозреваемым, потерпевшим, свидетелем) с технического, насыщенного жаргоном языка этих лиц на язык, понятный другим участникам судопроизводства (адвокату, прокурору, судье и т.д.).

Допрос эксперта производится, как правило, для разъяснения данного им заключения. В этом случае также функция допроса заключается не только в раскрытии существенных деталей, не отраженных в выводах эксперта или исследовательской части экспертного заключения, но и «переводе» написанного техническим языком на язык, понятный всем участникам судопроизводства.

4. Обыск

Обыск по своим информационно-познавательным целям весьма близок к следственному осмотру.

По делам о преступлениях в сфере предоставления услуг Интернета рассматриваемое следственное действие, как правило,

носит неотложный характер. Основанием для его производства является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела (ст. 182 УПК РФ).

Цели обыска: обнаружение, фиксация и изъятие перечисленных выше объектов, а также выявление и задержание разыскиваемых и подозреваемых лиц.

Обыск в необходимых случаях производится на квартире подозреваемого, месте его работы, а также в других местах, где он имел доступ к компьютерной технике.

Целями проведения обыска при расследовании преступлений, совершаемых с использованием высоких технологий и телекоммуникаций, являются обнаружение и изъятие (в случае возможности его осуществления) материальных объектов, способных по своим физико-техническим свойствам содержать информацию, имеющую отношение к расследуемому преступлению. К таким объектам могут быть отнесены:

- ✓ компьютерная техника или устройства (смартфоны, планшеты и т.д.);
- ✓ электронные носители информации;
- ✓ вспомогательные системы, обеспечивающие нормальное функционирование автоматизированных информационных систем (линии электропитания, заземления и т.д.);
- ✓ зафиксированные на бумаге алгоритмы, или иные записи преступников;
- ✓ справочная техническая литература, руководства по эксплуатации, технические журналы, блокноты и иные документы.

Существенной особенностью обыска при расследовании преступлении указанной выше категории является то, что следователь, проводящий данное следственное действие, как правило, не может оценить на месте значение обнаруживаемой информации, так как, во-первых, он сталкивается с огромными ее объема-

ми и, во-вторых, она представлена в специальном виде, для восприятия которого необходимы определенные специальные знания, иногда специальные аппаратные и программные средства.

В связи с этим наиболее целесообразным действием следователя при проведении обыска является изъятие всех обнаруженных электронных носителей информации или, по возможности, копирование такой информации.

На подготовительном этапе необходимо определить месторасположение и планировку помещения, которое должно быть подвергнуто обыску. Выяснить характер охраны объекта. Определить пути возможного отхода подозреваемого (обвиняемого). [1]

В практике расследования встречаются случаи использования обыскиваемым лицом специальной техники, обеспечивающей практически мгновенное гарантированное невосстановимое уничтожение информации с любого носителя, выполняемые как в стационарной комплектации, так и в мобильной.

Для устранения препятствий подобного рода необходимо использовать комплекс организационно-тактических мероприятий, включающий:

- ✓ четкое планирование действий членов СОГ;
- ✓ блокирование активных действий ответственных операторов;
- ✓ изъятие у операторов средств управления комплексами;
- ✓ отключение линий связи (телефония, Интернет);
- ✓ использование блокираторов радиосвязи в различных диапазонах;
- ✓ предотвращение отключения энергоснабжения, обеспечение охраны распределительного щита;
- ✓ запрет производить какие-либо манипуляции с компьютерами и носителями информации;

[1] Илюшин Д.А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг Интернет // Вестник Муниципального института права и экономики (МИПЭ). Вып. 1. Липецк: Интерлингва, 2004. С. 77 – 86.

✓ обеспечение отключения беспроводных систем передачи данных.

При наличии в осматриваемом помещении локальной сети необходимо точно установить местоположение серверов. Определить местоположение компьютеров при наличии локальной сети поможет проводка.

Следует обратить внимание на содержимое мусорных корзин, надписей и наклеек на мониторе и системных блоках, т.к. там могут содержаться данные о пароле и учетном имени (логине) пользователя.

Особое внимание нужно обратить на места хранения внешних носителей информации, данные о подключении таких носителей содержатся в служебных файлах и реестре операционной системы. Причем в качестве носителей информации могут выступать, например, фоторамки, плееры и другие мультимедийные устройства.

Все изъятые системные блоки должны быть опечатаны таким образом, чтобы исключить возможность их включения и разборки[1].

2.3. Особенности расследования краж и мошенничеств с использованием пластиковых карт и электронных платежных систем

Важной особенностью механизма следообразования по кражам и мошенничествам, совершенным с использованием банковских карт и их реквизитов, является одновременное возникновение следов преступления в нескольких местах. Они возникают в рамках системы оборота банковских карт и их реквизитов, элементами которой являются: платежные системы; банки-эмитенты, банки-эквайреры; процессинговые центры; расчетные банки; торгово-сервисные предприятия; держатели карт; оборудование и коммуникации, связывающие финансовые организации

[1] Баркалов Ю.М Актуальные проблемы информационной безопасности: методические рекомендации для стран СНГ. Воронеж, 2015.

между собой и с пунктами обслуживания карт. Во время проведения операций между участниками оборота банковских карт в автоматическом режиме осуществляется обмен информацией о проводимых транзакциях, что влечет за собой изменения на машинных носителях информации.

На стадии возбуждения уголовного дела при проверке сообщения о краже и мошенничестве рассматриваемого вида необходимо устанавливать следующие обстоятельства:

1) факт проведения транзакции и ее характеристика (времени, места совершения транзакции, способа транзакции и др.);

2) наличие и характеристику ущерба;

3) сведения о пострадавшем лице;

4) характеристику банковской карты и ее связь с пострадавшим лицом;

5) сведения о возможном совершении держателем конкретной операции с использованием банковской карты, о ее передаче другому лицу, о поручении держателем другому лицу провести транзакцию с использованием банковской карты или ее реквизитов.

Основными методами проверки сообщений о кражах и мошенничествах, совершенных с использованием банковских карт и их реквизитов, являются:

1) запросы в банки-эмитенты, эквайреры, платежные системы с целью получения документов, отражающих факты совершения транзакций;

2) объяснения, взятые у держателей и лиц, совместно проживающих с ними;

3) осмотры мест происшествий;

4) осмотры предметов и документов: банковских карт; копий заявлений держателей об опротестовании конкретных транзакций; копий анкет держателей; копий договоров о кредитовании и выдаче банковских карт; копий выписок по карточным счетам за определенный период; копий электронных журналов банкоматов, POS-терминалов;

5) криминалистические и компьютерные исследования.

На первоначальном этапе расследования, в зависимости от места совершения кражи и мошенничества, возникают следующие типичные ситуации:

1) имеются сведения о совершении кражи / мошенничества в месте, оборудованном банкоматом;

2) имеются сведения о совершении кражи / мошенничества в месте, где используется POS-терминал;

3) имеются сведения о совершении кражи / мошенничества с использованием сети Интернет.

Общими для разрешения данных следственных ситуаций будут являться следующие действия:

1) осмотр места совершения транзакции с целью собирания и исследования следов совершения кражи или мошенничества;

2) допрос держателя банковской карты об обстоятельствах оспоренной транзакции;

3) допрос лиц, совместно проживающих с держателем карты, об обстоятельствах оспоренной транзакции;

4) допрос представителей банка об особенностях проведения транзакций, а также о факте совершения кражи или мошенничества;

5) выемка банковской карты у держателя и последующий ее осмотр с целью фиксации ее реквизитов и обнаружения на ней следов преступления;

6) выемка документов, подтверждающих договорные отношения между банком и держателем банковской карты, а также факт опротестования конкретных транзакций.

К тактическим особенностям осмотра места происшествия по делам о хищениях указанного вида относятся:

1) необходимость привлечения специалистов в области бухгалтерского учета и компьютерных технологий;

2) избирательность в применении тактических приемов;

3) наличие у понятых опыта использования банковских карт.

Глава 3.
ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ПОЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ВЫСОКИХ ТЕХНОЛОГИЙ

3.1. Назначение экспертиз по уголовным делам о преступлениях, совершенных с использованием высоких технологий и телекоммуникаций

В соответствии с УПК РФ[1] экспертиза назначается в случаях, когда при производстве дознания, предварительного следствия и при судебном разбирательстве необходимы специальные познания в науке, технике, искусстве или ремесле.

По делам рассматриваемой категории существует постоянная необходимость использования в процессе расследования специальных познаний в области новых информационных технологий. Данные познания необходимы как для получения доказательств, так и для процессуального оформления документов, подготовленных средствами компьютерной техники, которые впоследствии могут играть роль доказательств.

В настоящее время с помощью судебной компьютерной экспертизы можно решать следующие задачи:

✓ воспроизводить и распечатывать всю или часть компьютерной информации (по определенным темам, ключевым словам и т. п.), содержащейся на машинных носителях, в том числе находя-

[1] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон РФ от 18.12.2001 № 174-ФЗ: ред. от 29.07.2017. Доступ из справ.-правовой системы «КонсультантПлюс». (дата обращения: 17.08.2017).

щейся в нетекстовой форме (в сложных форматах – в форме языков программирования, электронных таблиц, баз данных и т. д.);

✓ восстанавливать компьютерную информацию, ранее содержавшуюся на машинных носителях, но впоследствии стертую или измененную (модифицированную) по различным причинам;

✓ устанавливать дату и время создания, изменения (модификации), стирания, уничтожения либо копирования той или иной информации (документов, файлов, программ и т. д.);

✓ расшифровывать закодированную информацию, подбирать пароли и раскрывать систему защиты СВТ;

✓ исследовать СВТ на предмет наличия в них программно-аппаратных модулей и модификаций, приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ПК, системы ПК или их сети (вредоносных средств – компьютерных вирусов, «закладок», «жучков» и т. п.);

✓ определять авторство, место (средство) подготовки и способ изготовления документов (файлов, программ), находящихся на машинном носителе информации;

✓ выяснять возможные каналы утечки конфиденциальной информации из компьютерной сети, конкретных СВТ и помещений; устанавливать возможные несанкционированные способы доступа к охраняемой законом компьютерной информации и ее носителям;

✓ выяснять техническое состояние, исправность СВТ, оценивать их износ, а также индивидуальные признаки адаптации СВТ к конкретному пользователю;

✓ выяснять причины и условия, способствующие совершению правонарушения, связанному с использованием СВТ.

Также к задачам, которые следует решать с использованием возможностей судебно-компьютерной экспертизы, относятся: определение алгоритма вредоносной программы; извлечение из вредоносной программы списка управляющих серверов; доку-

ментирование функциональных особенностей вредоносной программы (например, особенностей ее взаимодействия с системами дистанционного банковского обслуживания); определение и документирование реализованных в программе способов противодействия криминалистическому исследованию и обнаружению; документирование изменений, вносимых программой в системный реестр и файловую систему в целом; определение и описание иных действий программы с информацией, которые могут иметь значение для уголовного дела; исследование конфигурационных файлов и дополнительных программных модулей, загружаемых вредоносной программой из сети Интернет; корреляция полученной информации с другими экземплярами вредоносных программ; установление абонентских номеров, с которых поступает SMS-сообщение со ссылкой на загрузку вирусной программой; установление интернет-сайта, с которого осуществлена загрузка вредоносной программы, а также IP-адреса, с которого вирусная программа поступила на сайт.[1]

Исходя из этих задач, ***следователь может поставить на разрешение эксперта следующие основные вопросы:***

✓ Является ли представленное на исследование техническое устройство средством электронно-вычислительной техники? Если да, то укажите тип, вид, назначение, техническое состояние и тактико-технические характеристики.

✓ Каковы тип, вид, марка, изготовитель, техническое состояние, тактико-технические характеристики (исправность, процент износа, и т. п.) средств вычислительной техники, представленных на исследование?

✓ Какая информация содержится на машинных носителях, представленных на исследование?

✓ Возможна ли раскодировка информации, записанной в сложных форматах? Если да, то каково ее содержание?

[1] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Указ. соч. С. 144-145.

✓Какие документы находятся на представленных на исследование машинных носителях информации? По возможности представьте их в виде распечатки на бумажном носителе.

✓Какая компьютерная информация и в какой форме (файл, программа, документ) была стерта, скопирована, изменена (модифицирована), уничтожена?

✓Каковы индивидуальные признаки компьютерной информации, представленной на исследование, - название, размер, дата и время создания, изменения (модификации)?

✓Когда и в какое время был создан файл (документ), представленный на исследование?

✓Как изменялось содержание обнаруженных документов (конкретных файлов, программ) на представленных на исследование машинных носителях информации - по названию, размеру, дате, времени создания (стирания, изменения)?

✓Возможно ли получение скрытой информации, касающейся проходящих по делу лиц (предметов, документов, событий)? Если да, то представьте ее в виде распечатки на бумажном носителе.

✓Изготовлены ли представленные документы с использованием печатающих средств компьютерной техники?

✓Содержатся ли на представленных на исследование средствах вычислительной техники программно-аппаратные модули и модификации, способные уничтожать, блокировать, модифицировать либо копировать информацию, нарушать работу ПК, системы ПК или их сети без предварительного предупреждения пользователя о характере действия или не запрашивающие разрешение пользователя на реализацию программой своего назначения? Если да, то какие? Каков характер их воздействия на ПК и ее программное обеспечение?

✓ Содержатся ли на представленных на исследование средствах вычислительной техники программно-аппаратные модификации, влияющие на конечные результаты работы конкретного технического устройства либо программного продукта? Если да,

то какие? Каков характер и последствия их воздействия на конкретное устройство и его программное обеспечение?

✓ Нарушение каких правил эксплуатации ПК, системы ПК, их сети, а также систем их безопасности привело к наступлению опасных последствий?

✓ Каким паролем (кодом) осуществляется доступ к ПК (системе ПК, компьютерной сети, программе, файлу, периферийному устройству и т. п.), представленному на исследование?

✓ Каковы тип, вид, марка, изготовитель, техническое состояние и основные тактико-технические характеристики средства защиты ПК (компьютерной информации), представленного на исследование?

✓ Каковы каналы утечки компьютерной информации из ПК, системы ПК, компьютерной сети, иного средства электронно-вычислительной техники, помещения, проходящих по делу?

✓ С помощью каких технических устройств было осуществлено копирование (стирание, уничтожение, модификация) охраняемой законом компьютерной информации? По возможности укажите тип, вид и основные тактико-технические характеристики устройства.

✓ Возможно ли сопряжение (соединение) представленного на исследование технического устройства с ПК, системой ПК или компьютерной сетью? Укажите тактико-технические характеристики аппаратуры.

Этот список вопросов не является исчерпывающим и может быть расширен, исходя из обстоятельств конкретного уголовного дела. В затруднительных случаях при постановке вопросов следует консультироваться у самого эксперта.

Постановление о назначении программно-технической экспертизы должно содержать максимально полную описательную часть, в которой следует отразить:

- обстоятельства уголовного дела;
- сведения о лицах, причастных к совершению преступления;

- документы, сведения о которых могут содержаться на машинных носителях, представляемых на исследование;

- сведения, которые могут быть использованы в качестве «ключевых» слов при восстановлении и(или) поиске экспертом информации (например, названия фирм, учреждений и организаций, фамилии клиентов, предполагаемые номера счетов и т. д.).

В резолютивной части объем задания эксперту должен быть определен конкретно. Современные СВТ имеют большие объемы постоянной памяти в виде жестких дисков, поэтому следователь физически не сможет изучить и оценить содержание всего машинного носителя в течение приемлемого для этого времени. Для оптимизации данного процесса темы интересующей следователя информации должны быть точно обозначены при постановке вопросов, а сами они - сформулированы кратко и информативно.

При постановке вопроса необходимо использовать устоявшийся понятийный аппарат, исключающий жаргонные и полупрофессиональные термины («винчестер», «логи», «взлом» и т.п.). В случае отсутствия терминов, определенных законодательными или нормативными актами, необходимо использовать те термины, которые употребляют разработчики технических средств, программных продуктов в документации, описаниях, справках и т.п.

К постановке вопросов предъявляются следующие требования:

✓ вопрос должен быть четким и однозначным;

✓ формулировка вопроса не должна касаться этапов исследования информации (описание характеристик носителей информации и особенностей размещения информации на них, восстановление и исследование информации среди удаленных файлов являются обязательным этапом исследования информации);

✓ вопросы не должны носить справочный характер;

✓ вопросы не должны носить правовой характер и выходить за пределы компетенции эксперта;

✓ вопросы должны соответствовать существующей методической и технической базе[1].

При назначении судебно-компьютерной экспертизы следователь должен четко представлять ее возможности и ограничения, не ставить перед экспертами вопросы и задания, выходящие за рамки их компетенции.

По делам рассматриваемой категории назначаются также: технологические, электроакустические, фоноскопические, видеофоноскопические, радиотехнические, электротехнические и иные технические экспертизы; в зависимости от отрасли хозяйства или характера нарушений - товароведческие, финансово - экономические, криминалистические экспертизы (в частности, технико-криминалистические экспертизы документов, по исследованию бумаги, чернил (красок), почерка и т. д.).

Например, при назначении радиотехнической экспертизы перед экспертом можно поставить следующие вопросы:

1. Является ли представленное на исследование устройство (самостоятельно или в комплекте) радиопередающей (радиоприемной) аппаратурой (установкой)?

2. В каком диапазоне радиочастот работает данное устройство и какова его мощность в антенне? Укажите дальность радиосвязи и другие тактико-технические характеристики приема/передачи.

3. В работе какого канала электросвязи используется данное устройство?

4. Является ли данное устройство самодельным, заводского изготовления или частью промышленной аппаратуры (ее отдельными блоками)?

[1] Баркалов Ю.М. Подготовка экспертов по производству компьютерных судебных экспертиз. Воронеж: Воронежский институт МВД России, 2013. С. 37.

5. Возможно ли использование данного устройства для проведения специальных технических мероприятий (разведывательных или контрразведывательных)?

6. Создает ли данное устройство помехи в каналах электросвязи, в частности, для радио- и телеприема (телефонной, телеграфной, факсимильной, связи ПК и др. видов электросвязи)? Если да, то насколько превышены допустимые нормы и к каким вредным последствиям может привести эксплуатация данного устройства?

Таким образом, наряду со штатными экспертами соответствующих учреждений правоохранительных органов, к подготовке и участию в следственных действиях необходимо шире привлекать специалистов профильных предприятий и учреждений, научно-исследовательских и учебных заведений, а также отдельных специалистов, имеющих опыт практической работы в определенной области знаний.

В настоящее время судебно-компьютерную экспертизу помимо территориальных подразделений ЭКЦ МВД России также можно поручить следующим организациям (учреждениям):

- ✓ АНО НИЦЭС - 121596, г. Москва, ул. Толбухина, д. 13/2, офис 5;
- ✓ АНО «Центр информационной безопасности, экспертизы и сертификации» - 127560, г. Москва, ул. Коненкова, д. 19 «Г», кв. 23 (Стоимость проведения исследования или экспертизы 1 объекта составляет 65 тысяч рублей);
- ✓ «Group-IB» - 115088 г. Москва, ул. Шарикоподшипниковская, д. 1, БЦ «Прогресс Плаза», 9 этаж (экспертиза 1 объекта составляет 300 000 рублей);
- ✓ ООО «Доктор Веб» - 125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12 «А»;
- ✓ «Лаборатории Касперского» - 125212, г. Москва, Ленинградское шоссе, д. 39 «А», стр. 3, БЦ «Олимпия Парк».

Здесь надо отметить, что следователям приходится сталкиваться с загруженностью государственных судебно-экспертных учреждений и, как следствие, несвоевременностью выполнения экспертиз. Однако, коль скоро следователи (дознаватели) вправе выбирать судебно-экспертное учреждение, в 58% случаев проведение экспертизы они поручали государственно-экспертным учреждениям и лишь в 5% - негосударственным. Объясняется это тем, что у негосударственных экспертных учреждений не всегда есть необходимое оборудование и средства для проведения судебной компьютерно - технической экспертизы. На это указали 40% опрошенных[1].

Следователь, правильно оценив и тщательно изучив заключения экспертов и прилагаемые к ним материалы, может широко использовать полученные данные как при назначении и производстве других экспертиз и следственных действий, так и в качестве самостоятельных доказательств по делу. Поэтому необходимо регулярное обеспечение следователей актуальной криминалистической информацией и необходимыми для успешной работы практическими навыками[2].

3.2. Особенности производства судебной компьютерной экспертизы по уголовным делам о преступлениях, совершаемых с использованием высоких технологий и телекоммуникаций

При производстве компьютерных экспертиз и исследований основным является обеспечение неизменности информации на исследуемых носителях информации. Для этого применяют аппаратные или программные средства блокирования записи.

[1] Шевченко Е.С. Актуальные проблемы расследования киберпреступлений // Эксперт-криминалист. 2015. № 3.

[2] Бутенко О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия // Lex russica. 2016. № 4.

В качестве существенного недостатка в деятельности подразделений ЭКЦ МВД России по делам данной категории стоит отметить недостаточное количество экспертов, имеющих допуск к проведению необходимых видов судебных компьютерно-технических экспертиз.[1]

При производстве судебной компьютерной экспертизы решают следующие задачи:

1. Поиск информации.

2. Определение обстоятельств установки и использования программных продуктов и оборудования.

К задачам поиска информации относят:

- поиск текстовой информации по ключевым словоформам;
- поиск графической информации по заданным критериям;
- поиск текстовой и графической информации по соответствию предоставленным образцам;
- поиск информации о сетевых подключениях (выход в сеть «internet»);
- поиск программных продуктов и др.

Для решения задачи поиска компьютерной информации вопросы, выносимые на компьютерную экспертизу, могут быть сформулированы следующим образом:

- имеется ли на представленных на исследование машинных носителях (дать перечень) информация, содержащая следующие ключевые слова: (дать перечень ключевых слов)?
- имеется ли на предоставленных на исследование машинных носителях (дать перечень) информация о (изложить о чем)?

Возможности экспертизы выявляют задачи, решаемые судебными экспертами этой области, определяют пределы (грани-

[1] Чекунов И.Г., Шумов Р.Н. Современное состояние киберпреступности в Российской Федерации. // Российский следователь. 2016. № 10.

цы) исследований, но не решают вопрос о возможности стандартизации (унификации) таких задач[1].

Перед началом поиска информации необходимо выполнить восстановление удаленной информации, при этом восстановление информации следует выполнять с использованием различных специализированных программных продуктов.

Поиск текстовой информации проводится по ключевым словам (приводятся в вопросах постановления о назначении экспертизы). Для поиска текстовой информации используются стандартные средства поиска «Windows», программы «Архивариус 3000», «AVSearch» и встроенные средства поиска файловых менеджеров.

Поиск графической информации проводится путем просмотра графических файлов. Важно заметить, что изображения также могут содержаться, например, в файлах, созданных приложениями Office, однако данные файлы графическими являться не будут. С помощью программ поиска текстовой информации возможно искать графические файлы, например, содержащие информацию EXIF. При этом возможно установить графические файлы, созданные с помощью определённых моделей цифровых фотоаппаратов или камер мобильных телефонов.

Для поиска графической информации с помощью «Архивариус 3000» возможно вводить в поисковый запрос сведения EXIF цифровой фототехники, например, модель или серийный номер цифровой фотокамеры.

Также возможен поиск по расширению файлов. Найденные файлы копируются на стендовый носитель для дальнейшего исследования (просмотра).

Определение обстоятельств установки и использования программных продуктов и оборудования проводится следующим образом:

[1] Хажевскас А., Гражялис К., Горбатков А. Актуальные проблемы проведения экспертизы информационных технологий. // Эксперт-криминалист. 2013. № 3.

- исследуется установленное программное обеспечение на контрафактность;
- проверяются параметры и регистрационные данные программного обеспечения;
- поиск следов использования программного обеспечения и оборудования.

В среде «Windows» большинство основных данных об установленном программном обеспечении и оборудовании хранится в реестре.

Для просмотра файлов журналов событий можно использовать штатные средства операционной системы, в меню «действия» программного обеспечения «управление компьютером», открыв исследуемый файл. Или воспользоваться специализированным программным обеспечением, например «Event Log Explorer».

Для определения проведенных действий операционной системой семейства «Windows» производится просмотр журналов событий операционной системы.

В «WindowsXP» данные файлы по умолчанию расположены в директории «%SYSTEMROOT%\system32\config\ и имеют расширение «.Evt»

Для Windows 7 данные файлы по умолчанию расположены в директории «%SYSTEMROOT%\System32\Winevt\Logs\» и имеют расширение «.Evtx».

Просмотром данного журнала возможно определить:

✓ временные рамки работы операционной системы;

✓ временные рамки запуска ряда программных продуктов, запуск которых отображается в журнале событий операционной системы «Windows»;

✓ временные рамки подключения – отключения сетевых ресурсов (сетевого адаптера), запуск которых отображается в жур-

нале событий операционной системы «Windows», и ряд других параметров.

К программным продуктам, которые оставляют различные следы при работе в операционных системах, относятся:

- ✓ браузеры (Internet Explorer, Opera, Mozila Firefox, Google Chrome идр.);
- ✓ программы для переписки (ICQ, QIP, Skype и д.р.);
- ✓ программы – почты (Outlook Express, The Bat);
- ✓ другие программы – игры, торенты и т.д.

При работе в браузерах следы остаются в файлах cookies, cache браузера и реестре.

Частные требования:

1. Вопросы должны быть направлены на установление конкретных обстоятельств расследуемого события.

2. Вопросы должны быть поставлены так, чтобы при решении конкретных задач расследования затраты (финансовые, технические, временные и пр.) на проведение исследований были минимальными.

3. Вопросы должны соответствовать уровню подготовки и инструментальному оснащению экспертов того экспертного учреждения, которому назначается экспертиза.

4. Вопросы должны соответствовать представляемым на исследование вещественным доказательствам.

При постанове вопросов о работоспособности программного обеспечения можно сослаться на ГОСТ 28195-89 (Оценка качества программных средств. Общие положения).

Под «работоспособностью программного средства» понимается «способность программы функционировать в заданных режимах и объемах обрабатываемой информации в соответствии с программными документами при отсутствии технических средств».

Для решения данного вопроса необходим весь комплект документации по рассматриваемому программному обеспечению. При этом продукт должен содержать все задекларированные разработчиком возможности, которые известны только разработчику[1].

Последовательность действий эксперта

Действия эксперта должны проводиться в следующем порядке:

1. Осмотреть и описать упаковку объектов, представленных на экспертизу. Опционально – сфотографировать упаковку.

2. Извлечь объекты из упаковки, сфотографировать (с линейкой) и описать.

3. При описании системного блока привести:

✓ габаритные размеры (ширина х, высота х, глубина в мм);

✓ цвет корпуса;

✓ расположение и описание устройств, кнопок, индикаторов, разъемов, наклеек на передней панели (лицевой стороне) системного блока;

✓ описание разъемов, наклеек и т.п. на задней панели (тыльной стороне) системного блока;

✓ описание боковых панелей системного блока (при наличии на них кнопок, разъемов и т.п.);

✓ описание индивидуализирующих особенностей (надписей, наклеек, повреждений и т.п.);

✓ описание основных компонентов системного блока (маркировочных обозначений на системной плате, платах расширения и пр.);

✓ сфотографировать системный блок со снятой боковой крышкой.

4. Извлечь из системного блока машинные носители и описать их. При описании указать:

✓ размерные характеристики (форм-фактор);

✓ основные маркировочные обозначения на НЖМД (марка, модель, емкость, серийный номер).

[1] Баркалов Ю.М. Подготовка экспертов по производству компьютерных судебных экспертиз. Воронеж: Воронежский институт МВД России, 2013. С. 50-53.

5. Просмотреть настройки даты и времени на системной плате с помощью базовой системы ввода-вывода (BIOS) и сопоставить их с текущими с указанием установленного и текущего часовых поясов.

При ответах на поставленные вопросы необходимо:

✓ выявить программное обеспечение, работа которого требует регистрации в операционной системе;

✓ выявить программное обеспечение, работа которого не требует установки в операционной системе;

✓ выявить удаленное программное обеспечение либо сведения, оставшиеся в операционной системе от ранее установленного и впоследствии удаленного программного обеспечения;

✓ описать и просмотреть наличие и содержимое возможных мест расположения следовой информации на машинных носителях.

При необходимости сопоставить найденную информацию между собой на предмет ее непротиворечивости и последовательности по времени.

6. Формулирование выводов эксперта.

По результатам исследования согласно ст. 204 УПК РФ составляется заключение эксперта[1]. Заключение судебной компьютерной экспертизы, показания эксперта, подтвердившего выводы проводимой им экспертизы, служат доказательствами виновности или невиновности подсудимых.[2]

Выводы должны соответствовать поставленным вопросам.

Количество выводов должно соответствовать количеству вопросов.

[1] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон РФ от 18.12.2001 № 174-ФЗ: ред. от 29.07.2017. Доступ и СПС «КонсультантПлюс». (дата обращения 17.08.2017).

[2] Добровольский В.И. Мошенничество в сфере кредитования и смежные составы преступлений: вопросы применения и разграничения ст. ст. 159.1, 159.3 УК РФ и иных составов преступлений (подготовлен для системы КонсультантПлюс, 2014)

ЗАКЛЮЧЕНИЕ

Киберпреступность – это сходная группа общественно опасных деяний, посягающих на общественную безопасность, собственность, права человека, другие охраняемые законом отношения, необходимым элементом механизма подготовки, совершения, сокрытия и отражения которых является компьютерная информация, выступающая в роли предмета и средства преступления.

По данным исследований, прогнозируется уменьшение количества использования преступниками вредоносных программ (троянские программ) для хищения с банковских счетов путем модификации информации (подделка электронных платежных документов), а также уменьшение количества использования преступниками специальных технических средств (скимминг и т.п.) для хищения денежных средств путем копирования информации платежных карт в POS-терминалах и банкоматах. При этом прогнозируется увеличение количества используемых преступниками вредоносных программ (троянские программ) для хищения с банковских счетов путем копирования информации (данных банковских карт, логинов и паролей для интернет-банкинга), находящейся в мобильных устройствах на платформе Android, вредоносных программ для хищения с банковских счетов путем модификации, копирования и уничтожения информации (подделка электронных платежных документов), находящейся в банковской системе (банковских компьютерах), будет увеличиваться количество вредоносных программ (троянские программы) для хищения денежных средств путем модификации и копирования информации платежных карт в POS-терминалах и банкоматах.

Подводя итоги всему изложенному, скажем, что раскрытие и расследование киберпреступлений остается довольно сложной задачей для большинства сотрудников органов предварительного расследования. Это отчасти обусловлено отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях.

Как показало исследование научной литературы и опрос следователей (дознавателей), для решения приведенных проблем и повышения эффективности расследования киберпреступлений необходимо: повысить уровень мониторинга данного вида преступлений; разработать программы повышения квалификации следователей (дознавателей) по расследованию данной категории дел; повысить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий; увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования киберпреступлений.

ТЕРМИНОЛОГИЧЕСКИЙ СЛОВАРЬ

IP-адрес – это уникальный сетевой адрес узла (компьютера) в компьютерной сети, построенной по протоколу IP. Каждый компьютер, если соблюдается протокол IP, в любой сети, в том числе в сети Интернет, имеет свой индивидуальный IP-адрес, который выглядит в виде 4 групп комбинаций цифр (например, 193.233.5.231). Для выхода в сеть IP-адрес является обязательным атрибутом.

MAC-адрес – это уникальный идентификатор, встроенный в сетевую карту оборудования (сотовый телефон, компьютер, планшет). MAC-адрес является индивидуальным и присваивается производителем сетевой карты. МАК-адрес не меняется и является постоянным для отдельно взятой единицы оборудования и в обязательном порядке прописывается на сервере интернет-провайдера, предоставляющего доступ к сети Интернет.

Web-ресурс (Web(Интернет)-ресурс) – это информационная система, использующая (Web(Интернет) технологии на уровне представления и передачи данных, предназначенная для оказания публичных информационных услуг в сети Интернет. Работает на основе клиент-серверного принципа. Пример: пользователь при помощи клиент программы – браузера запрашивает web-страницу rambler.ru. web-сервер обрабатывает запрос пользователя и направляет, при помощи сети Интернет, на данную страницу.

Cookies («куки») – это текстовые файлы, содержащие информацию о работе браузера, в том числе данные о посещении ресурсов и «кэши» паролей обращения к сетевым ресурсам.

Tor браузер – свободное и открытое программное обеспечение для реализации второго поколения так называемой луковой

маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Авторизация – это предоставление определенному лицу или группе лиц прав на выполнение определенных действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

Анонимайзер – изначально средство для скрытия информации о компьютере или пользователе в сети от удалённого сервера.

Аутентификация (*authentication*) – процедура проверки подлинности данных и субъектов информационного взаимодействия.

Виртуальные валюты – валюта, которую мошенники предпочитают использовать для оплаты приобретенных незаконных товаров и услуг в сети. Bitcoin также стал стандартным платежным решением при требовании выкупа и других форм вымогательства.

Дистанционное банковское обслуживание (ДБО) – общий термин для технологий предоставления **банковских** услуг на основании распоряжений, передаваемых клиентом.

Домен (доменное имя) – имя, предназначенное для идентификации областей автономии в сети Интернет. В сети Интернет имеется несколько доменных зон. В качестве примера одной доменной зоны можно обозначить web-адреса, имеющие домен I-го уровня: «ru», «com» и т.д. Все предшествующие указанному окончанию символы и значения составляют полное доменное имя, например www.yandex.ru.

Журнал событий (англ. **Event Log)** – в Microsoft Windows стандартный способ для приложений и операционной системы записи и централизованного хранения информации о важных программных и аппаратных событиях. Служба журналов событий сохраняет события от различных источников в едином журнале событий, программа просмотра событий позволяет

пользователю наблюдать за журналом событий, программный интерфейс (API) позволяет приложениям записывать в журнал информацию и просматривать существующие записи.

Интернет-провайдер (иногда просто провайдер) — организация (оператор связи), предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги.

Интернет-мошенничество - мошенничество с использованием глобальной сети Интернет.

Контент – это собирательный термин для любой информации, которая содержится в информационном ресурсе - тексты, фотографии, картинки, видео и аудиофайлы.

Компью́терный ви́рус (вирусная программа) – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

Маршрутизатор (роутер) – в бытовом варианте является устройством, обеспечивающим подключение нескольких компьютеров к сети Интернет. При этом маршрутизатор присваивает самостоятельный IP-адрес (локальный IP-адрес) подключённому к созданной им локальной сети устройству, а сам получает IP-адрес от интернет-провайдера. При этом маршрутизатор может иметь ряд вспомогательных функций, например, оснащён точкой доступа Wi-Fi для подключения устройств, использующих Wi-Fi соединения, в том числе в качестве маршрутизатора может выступать мобильное устройство, оснащённое этой функцией.

Мобильный банк – это простой и удобный sms-сервис, позволяющий получать информацию обо всех операциях по картам,

а также совершать платежи, переводы и другие операции с помощью мобильного телефона в любое время и в любом месте.

Никнейм («кличка», «прозвище») – это сетевое имя, псевдоним, используемый пользователем в сети Интернет при регистрации на различных web-ресурсах, обычно при общении в форумах, чатах и т.д.

Оператор платежной системы – юридическое лицо, определяющее правила платежной системы и выполняющее обязанности, предусмотренные Федеральным законом «О национальной платежной системе» от 27 июня 2011 года №161-ФЗ.

Оператор связи – это юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии.

Платёжная систе́ма – совокупность правил, процедур и технической инфраструктуры, обеспечивающих перевод стоимости от одного субъекта экономики другому. Платёжные системы являются одной из ключевых частей современных монетарных систем.

Сайт (часть сети) – это система электронной информации, созданной частным лицом или организацией в глобальной сети Интернет, объединённая одним адресом (доменным именем) и обеспеченная доступом пользователей сети к этой информации.

Сервер – мощный компьютер, обеспечивающий обмен информацией между клиентом (компьютером пользователя) и сервером при помощи сети Интернет.

Удаленный доступ – технология взаимодействия абонентских систем с локальными сетями через территориальные коммуникационные сети. Удаленный доступ осуществляется посредством сервера удаленного доступа. При удаленном доступе используются модели "дистанционного управления" и "удаленной системы".

Хостинг – предоставление вычислительных возможностей для размещения информации на сервере в качестве услуги за вознаграждение. Обратившийся в адрес владельца хостинга заказчик

размещает на его сервере доступ к web-ресурсам, принадлежащим заказчику.

Электронный кошелек – компьютерная программа, позволяющая хранить электронные деньги, а также производить с их помощью безналичные расчеты в сети Интернет. По сути, электронный кошелек выступает аналогом банковского счета.

Автозалив - жертва лично создает необходимое ей платежное поручение и нажимает отправку в банк платежного поручения. В этот момент вирус автоматически заменяет данные в платежном поручении на указанные злоумышленником. В данном случае злоумышленник на ПК жертвы никак не воздействует.

Бот-сети (botnets) – сети зомбированных (инфицированных) компьютеров. Зараженный компьютер-бот в дальнейшем используется для рассылки спама, проведения «атак на отказ в обслуживании» (Distributed Denial of Service - DDoS).

Кардинг – жаргонное название преступлений с банковскими картами – в них незаконно используются сами карты или информация о них. Различают «кардинг-он-лайн», включающий применение скомпрометированных карт в интернет-магазинах, «кардинг-офф-лайн» – использование карт для расчета в традиционных торгово-сервисных предприятиях (ТСП) и «кэшинг» – съем денег в банкомате (АТМ) по скомпрометированным картам. Занимаясь кардингом, можно либо получить информацию о реальной карте, либо сгенерировать все эти данные. Интересующиеся могут свободно найти ссылки на сайты, которые открыто торгуют сведениями о банковских картах.

Подделка карты – изготовление карт, реквизиты которых полностью повторяют реквизиты реальных карт, выпущенных эмитентом. По поддельному «пластику» можно совершать операции, выдавая его за настоящий.

Скимминг (skimming) – незаметное для держателя реальной карты копирование данных с магнитной полосы с помощью специальных устройств на банкомат, собираются данные клиен-

тов банка, которые воспользовались данным банкоматом. После чего на специальную заготовку записывается дамп карты потерпевшего и снимаются деньги прямо в банкомате, т.к. скимер списывает данные с карты и записывает пин-код к ней.

Скимминговое оборудование – оборудование для несанкционированного считывания информации с банковских карт физических лиц и фиксации ПИН-кодов к ним.

Сниффер (от англ. to sniff – нюхать) – программа или устройство для перехвата и анализа сетевого трафика (своего и/или чужого). Сниффер может анализировать только то, что проходит через его сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются всем машинам, из-за этого возможно перехватывать чужую информацию. Использование коммутаторов (switch, switch-hub) и их грамотная конфигурация уже является защитой от прослушивания. Между сегментами информация передаётся через коммутаторы. Коммутация пакетов — форма передачи, при которой данные, разбитые на отдельные пакеты, могут пересылаться из исходного пункта в пункт назначения разными маршрутами. Так что если кто-то в другом сегменте посылает внутри него какие-либо пакеты, то в ваш сегмент коммутатор эти данные не отправит.

Снять дамп карты – т.е. данные с магнитной ленты карты. После чего записать на заготовку карты, на которой принтером наносится изображение какого-либо банка и иногда эмбасируется номер карты и имя владельца, и в дальнейшем приобретаются какие-либо товарно-материальные ценности, так как не во всех терминалах нужен пин-код карты.

Фарминг – метод онлайнового мошенничества, заключающийся в изменении *DNS* (*Domain Name System*) адресов так, чтобы веб-страницы, которые посещает пользователь, были не оригинальными, а другими, специально созданными кибермошенниками для сбора конфиденциальной информации. Необ-

ходимая для инфицирования программа-вирус скрытно устанавливается на каждый компьютер бот-сети.

Фишинг (phishing – производное от phone –телефон и fishing – рыбалка) – преступление, в котором все персональны данные о картах и счетах клиента добываются злоупотреблением доверием (мошенничеством) - всю требуемую информацию владельцы карт передают преступникам добровольно. Часто фишинг осуществляется рассылкой по электронной почте официального письма якобы от имени представителя банка.

Дропы – играют важную роль в киберпреступлениях, именно они превращают похищенные логины и PIN-коды в реальные деньги. Работа дропа наиболее опасна - дроп снимает деньги в банкомате и затем передает их заказчику.

Кодеры – квалифицированные программисты, изготавливающие преступные инструменты - программы-вирусы, пользовательские боты, программы для рассылки спама и др. Часто кодеры предлагают сами преступные услуги. Поставляя программы, кодер минимизирует риск быть наказанным.

Кракеры (*crackers*) — специалисты, способные снять защиту от копирования с лицензионного программного обеспечения.

Хакеры — лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций.

Хактивисты – используется для обозначения явления социального протеста, которое представляет собой своеобразный синтез социальной активности, преследующей цель протеста против чего-либо, и хакерства (использования интернет-технологий с целью причинения ущерба компьютерным сетям и их пользователям).

СПИСОК ЛИТЕРАТУРЫ

а) нормативные правовые акты:

1. Конвенция о преступности в сфере компьютерной информации (ETS № 185) : заключена в г. Будапеште 23.11.2001 : с изм. от 28.01.2003.

2. Преступления, связанные с использованием компьютерной сети / Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями // A / CONF.187/10 // Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

3. Решение № 475 Межгосударственного Совета Евразийского экономического сообщества «О Концепции создания Евразийской инновационной системы» : принято в г. Санкт-Петербурге 11.12.2009 // Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

4. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

5. Конституция Российской Федерации // Собрание законодательства РФ. – 2014. – № 9. – Ст. 851.

6. Уголовно-процессуальный кодекс Российской Федерации // Собрание законодательства РФ. - 2001. - № 52 (часть I). - Ст. 4921.

7. Уголовный кодекс Российской Федерации // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

8. О национальной платежной системе : Федеральный закон РФ от 27 июня 2011 г. № 161-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 27. – Ст. 3872.

9. О персональных данных : Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31 (часть I). – Ст. 3451.

10. Об информации, информационных технологиях и о защите информации : Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31 (часть I). – Ст. 3448.

11. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон РФ от 26.07.2017 № 187-ФЗ // Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

12. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 // Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

б) основная литература:

1. Шмонин А.В. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий / А.В. Шмонин, Е.А. Ефремова, В.В. Баранов, А.В. Казюлин. – М., 2016. – 189 с.

2. Баркалов Ю.М. Актуальные проблемы информационной безопасности: методические рекомендации для стран СНГ/ Ю.М. Баркалов. – Воронеж, 2015.

3. Баркалов Ю.М. Подготовка экспертов по производству компьютерных судебных экспертиз / Ю.М. Баркалов. – Воронеж : Воронежский институт МВД России, 2013. – 65 с.

4. Яковлев А.Н. Особенности расследования преступлений, совершаемых с использованием электронных платежных средств и систем : научно-методическое пособие. / А.Н. Яковлев, Н.В. Олиндер. – М., 2012.

5. Яблоков Н.П. Криминалистика : учебник / Н.П. Яблоков – М. : ЛексЭст, 2006.

6. Осмотр места происшествия : практическое пособие / под ред. А. И. Дворкина. – М. : Юристъ, 2001.

7. Васильев А.Н. Тактика отдельных следственных действий / А.Н. Васильев. – М., 1981.

8. Райзберг Б.А. Современный экономический словарь / Б.А. Райзберг, Л.Ш. Лозовский, Е.Б. Стародубцева. – 6-е изд., перераб. и доп. – М.: ИНФРА-М, 2011.

в) дополнительная литература:

1. Ревенков П.В. Управление рисками в условиях электронного банкинга : автореф. дис. ... д-ра эконом. наук / П.В. Ревенков. – СПб., 2013.

2. Выборнов А. Устранение уязвимостей / А. Выборнов // BIS journal. – 2014. – № 4.

3. Лузгин И.И. Технико-криминалистическое обеспечение как мегаинструментальная технология формирования единого криминалистического пространства / И.И. Лузгин // Эксперт-криминалист. – 2010. – № 1. – С. 30 – 34.

4. Пропастин С.В. Следственный осмотр: проблема определения целей и задач / С.В. Пропастин // Современное право. – 2012. – № 5. – С. 133-135.

5. Яковлев А.Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: "электронная почта" / А.Н.

Яковлев // Вестник Воронежского института МВД России. – 2014. – № 4. – С. 46.

6. Илюшин Д.А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг Интернет / Д.А. Илюшин // Вестник Муниципального института права и экономики (МИПЭ). Вып. 1. – Липецк : Интерлингва, 2004. – С. 77 – 86.

7. Шевченко Е.С. Актуальные проблемы расследования киберпреступлений / Е.С. Шевченко // Эксперт-криминалист. – 2015. – № 3.

8. Бутенко О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия / О.С. Бутенко // Lex russica. – 2016. – № 4.

9. Чекунов И.Г. Современное состояние киберпреступности в Российской Федерации. / И.Г. Чекунов, Р.Н. Шумов // Российский следователь. – 2016. – № 10.

10. Хажевскас А. Актуальные проблемы проведения экспертизы информационных технологий / А. Хажевскас, К. Гражялис, А. Горбатков // Эксперт-криминалист. – 2013. – № 3.

11. Добровольский В.И. Мошенничество в сфере кредитования и смежные составы преступлений: вопросы применения и разграничения ст. 159.1, 159.3 УК РФ и иных составов преступлений / В.И. Добровольский. – Подготовлено для системы КонсультантПлюс, 2014.

г) интернет - источники:

1. Греф: необходимо создать систему по борьбе с киберпреступниками. – URL : http://ria.ru/economy/20160412714092152 02. html (дата обращения: 28 июля 2017 г.)

2. Безопасность банковских карт : взгляд потребителя и активность игроков рынка. Отчет по результатам исследования. – М.: Национальное агентство финансовых исследований, 2017. – URL : http://nacfin.ru/wpcontent/uploads/2017/01/moshennichestvo_ bankovskie_karty.pdf.

3. Попова Н. Российские банкоматы оказались в ливанской петле / Н. Попова // АН-online. – 2012. – 11 фев. – URL : http://argumenti.ru/crime/2012/02/156477, свободный.

4. Козловский В. Масштабы кибермошенничества растут / В. Козловский // Российская газета. – 2012. – 29 нояб. – URL : http://www.rg.ru/2012/11/29/karti-site.html, свободный.

Учебное издание

Наиля Рашидовна Шевко
Адель Миннурович Каримов
Елена Эдуардовна Турутина

Преступления, совершаемые с использованием высоких технологий и коммуникаций

Учебное пособие

Корректор Н.А. Климанова
Технический редактор Е.В. Зотина

Подписано в печать 16.11.2017 Усл.печ.л. 5
Формат 60х84 1/16 Тираж 30

Типография КЮИ МВД России
420108, г. Казань, ул. Магистральная, 35