ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ ПРОТИВ СОБСТВЕННОСТИ

Учебное пособие

Московский университет МВД России
имени В.Я. Кикотя

ISBN 978-5-9694-0845-6

Москва
2020

ББК 67.4
Р24

Рецензенты:
заместитель начальника Управления уголовного розыска ГУ МВД России по Московской области, кандидат юридических наук **П. В. Эзрохин**;
начальник организационно-зонального отдела СУ УМВД России по Белгородской области **И. М. Горбатых**

Коллектив авторов:
А. В. Пузарин, О. В. Химичева, А. В. Андреев, В. В. Гончар, К. Р. Аветисян, А. В. Долбилов, А. П. Дмитренко, Д. Н. Захаров, В. Ю. Иванов, Е. А. Русскевич, А. Ю. Молянов, В. Г. Любан

Р24 **Расследование преступлений в сфере компьютерной информации, совершаемых против собственности** : учебное пособие / [А. В. Пузарин и др.]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2020. – 185 с. − 1 электронный опт. диск (CD-R). − Систем. требования: CUP 1,5 ГЦ ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жестком диске.
ISBN 978-5-9694-0845-6

В учебном пособии рассмотрены основные вопросы, связанные с особенностями расследования преступлений в сфере компьютерной информации, совершаемых против собственности.

Авторский коллектив выделяет комплексный подход к подготовке специалистов органов внутренних дел, занимающихся противодействием преступлениям в сфере компьютерной информации, совершаемых против собственности. Отражены уголовно-правовые, уголовно-процессуальные, криминалистические, организационно-правовые и организационно-технические аспекты деятельности сотрудников правоохранительных органов по противодействию указанному виду преступлений.

Пособие ориентировано на преподавателей и студентов образовательных учреждений юридического и технического профиля, а также работников органов предварительного расследования.

ББК 67.4

ISBN 978-5-9694-0845-6

Научное электронное издание

Редактор *Абилова Ф. А.*
Компьютерная верстка *Абилова Ф. А.*
10,84 усл. печ. л.

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
http://www.mosu.mvd.ru, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информационные технологии и программное обеспечение достаточно прочно проникли во все сферы жизнедеятельности человечества. Мы используем их и на работе, и в быту, совершаем покупки и платежи, учимся, получаем, храним и делимся информацией с коллегами, друзьями и родственниками, создаем и распространяем интересные и полезные информационные продукты. Сейчас любое техническое средство обработки информации, по сути, представляет собой микрокомпьютер, который выполняет заданную программистом последовательность операций, зачастую имеет интерфейс взаимодействия с пользователем и, как правило, работает совместно с другими такими же средствами, обмениваясь информационными пакетами данных и образуя единое информационное пространство. При этом информация, представленная в цифровом виде, накапливается, хранится, подвергается различным модификациям и передается по всевозможным каналам связи на другие устройства.

Информация, информация, информация! Она окружает нас со всех сторон: мы стремимся ее получить, делимся с другими, преобразуем к нужному и удобному для восприятия виду, используем в различных целях, сохраняем на время, ограничиваем к ней доступ, удостоверяемся в ее целостности, конфиденциально передаем по открытым каналам связи.

Информационные технологии удовлетворяют потребностям самого привередливого пользователя: в настоящее время созданы и совершенствуются информационные ресурсы практически во всех сферах деятельности человека, позволяя в кратчайшие сроки решать самые разнообразные задачи.

При этом следует отметить, что развитие информационного пространства и использование его в благих целях активизировало деятельность ряда недобросовестных личностей и групп, которые в погоне за легкой наживой стали совершать «компьютерные преступления», совокупность которых уже имеет свое собственное, известное во всем мире название – «киберпреступления», а данное явление получило наименование «киберпреступность».

Высокие темпы роста преступных посягательств в сфере информационных технологий, совершаемых в том числе против собственности, выявили множество проблемных вопросов. Как квалифицировать то или иное деяние? Как его вообще понять, распознать, именовать? Как найти, зафиксировать и задокументировать следы преступления в цифровом мире? Как выявить по конкретному киберпреступлению причастных лиц? Как доказать их причастность, виновность или невиновность? Эти и множество других вопросов продиктованы действительностью и требуют скорейшего разрешения.

Решение данных вопросов, по нашему мнению, необходимо начать с детального исследования феномена «киберпреступности», концентрации внимание законодателей, правоприменителей и технических специалистов на проработке юридических аспектов, относящихся к данной сфере, созданию и развитию соответствующей базы знаний, обеспечению специалистов всех уровней единой терминологией, а также сбору и поддержке в актуальном состоянии всех необходимых организационных, технических и специальных познаний, требующихся для предупреждения, расследования и раскрытия преступлений подобного рода.

Определенная работа в этом направлении уже проделана. Получен достаточный опыт в расследовании и раскрытии киберпреступлений, с привлечением виновных к ответственности. Однако ряд актуальных проблем до сих пор остаются нерешенными: об этом мы и поговорим на страницах данного пособия.

ГЛАВА I. АКТУАЛЬНЫЕ ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ ПРОТИВ СОБСТВЕННОСТИ

§ 1.1. Уголовно-правовая характеристика отдельных видов преступлений

Вопросы законодательного определения и практического применения уголовно-правовых норм об ответственности за преступления в сфере компьютерной информации достаточно активно разрабатываются в отечественной доктрине уголовного права[1]. Вместе с тем следует признать, что практику их применения до настоящего времени нельзя признать удовлетворительной, хоть в малой степени соответствующей современному масштабу криминальной активности в виртуальном пространстве.

По данным ГИАЦ МВД России динамика преступлений, предусмотренных гл. 28 Уголовного кодекса Российской Федерации (далее – УК РФ), представлена следующим образом (рис. 1.1):

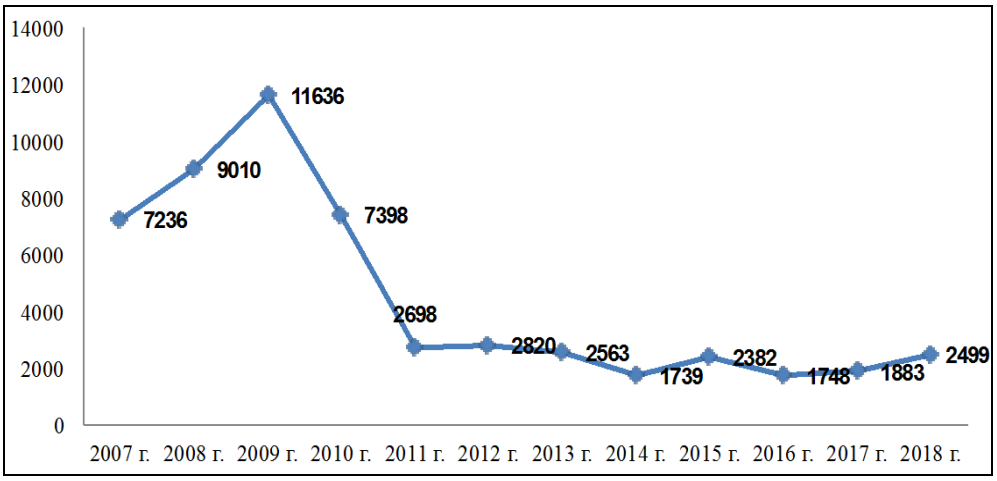

Рис. 1.1. Количество преступлений по статьям, включенным в главу 28 УК РФ

Статьей 272 УК РФ предусмотрена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (рис. 1.2).

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

---

[1] Будаковский Д. С. Способы совершения преступлений в сфере компьютерной информации // Российский следователь. – 2011. – № 4 ; Гостева М. Б. Преступления в сфере компьютерной информации: проблемы и недостатки новой редакции // Проблемы права. – 2012. – № 5 ; Халиуллин А. И. Вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации // Труды Академии управления МВД России. – 2011. – № 4.

В теории уголовного права нет общепринятой позиции относительно ключевого вопроса о том, что следует понимать под «охраняемой законом информацией»[1]. Высказана точка зрения, что неправомерный доступ к компьютерной информации имеет место при обращении к любой информации вопреки воли ее владельца[2], а предметом анализируемого преступления является компьютерная информация, в отношении которой собственник явным образом объявил об ограничениях по ее использованию[3].

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

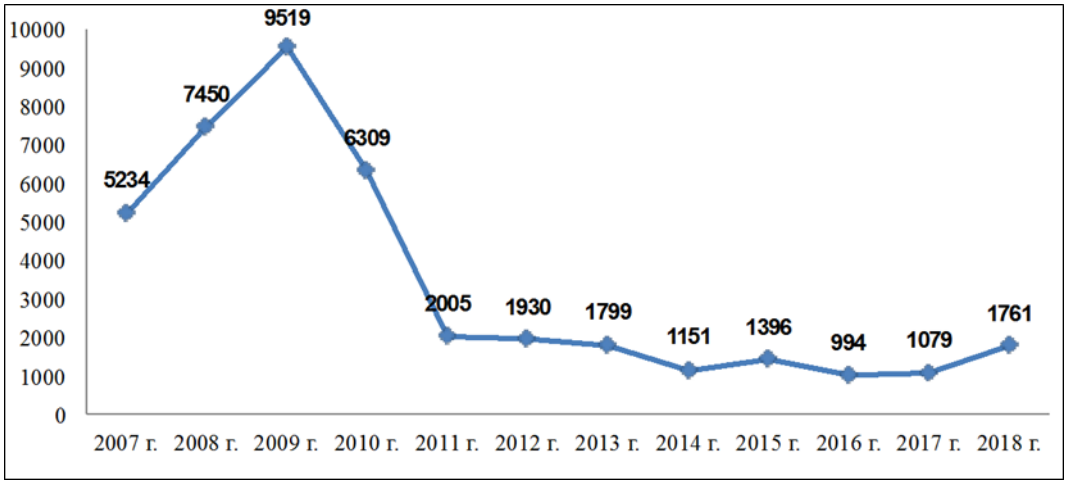

Рис. 1.2. Количество зарегистрированных преступлений по ст. 272 УК РФ

Вместе с тем все большее распространение стала получать позиция, согласно которой под «охраняемой законом информацией» следует понимать лишь, так сказать, закрытую информацию, к которой относятся государственная, служебная, коммерческая, банковская, врачебная, нотариальная, адвокатская тайны, персональные данные и т. д.[4] В Методических рекомендациях Генеральной прокуратуры Российской Федерации, в частности, указано, что по смыслу ст. 272 УК РФ охраняемой законом информацией являются лишь сведения, в отношении которых установлен специальный режим правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т. д.)[5].

Отсутствие общепринятого толкования термина «охраняемая законом информации» закономерно обусловило неединообразную практику применения ст. 272 УК РФ. Отдельные суды, придерживаясь рекомендаций Генеральной прокуратуры Российской

---

[1] Следует отметить, что законодательства ряда стран используют более общую категорию – «информация, хранящаяся в компьютерной системе, сети или на машинных носителях» ; Швед Н. А. Неправомерный доступ к компьютерной информации: уголовно-правовая защита в Российской Федерации и Республике Беларусь // Информационное право. – 2016. – № 2. – С. 32.

[2] Доронин А. М. Уголовная ответственность за неправомерный доступ к компьютерной информации : автореф. дис. … канд. юрид. наук. М., 2003. С. 6.

[3] Малышенко Д. Г. Уголовная ответственность за неправомерный доступ к компьютерной информации : дис. … канд. юрид. наук. М., 2002. С. 58.

[4] Гузеева О. С. Квалификация преступлений в сфере компьютерной информации. М., 2016. С. 30.

[5] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». URL: https://www.consultant.ru.

Федерации, указывают, что неправомерные манипуляции с открытой (общедоступной) информацией не подпадают под действие данной статьи.

Так, отменяя обвинительный приговор, вышестоящий суд указал: «…По смыслу закона под охраняемой законом понимается информация, для которой установлен специальный режим ее правовой защиты… то есть информация ограниченного доступа… При этом судом сделаны выводы, что указанная информация (новости, советы логопеда, психолога и т. п.) охраняется законом – ст. 6 Федерального закона от 27 июня 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Однако данные выводы противоречат содержанию вышеуказанных законодательных актов Российской Федерации. Информация на сайте, в редактировании и удалении которой признана виновной К., является общедоступной информацией, к которой относятся общеизвестные сведения и для которой отсутствует необходимость установления специального режима ее правовой защиты. Указанное закреплено в пп. 1.7 и 3.2. Положения о сайте МБДОУ «1», утвержденного приказом заведующей учреждения, согласно которому информационный ресурс сайта является открытым и общедоступным, информация на сайте является открытой и общедоступной, если иное не определено специальными документами. При этом таковых в материалах уголовного дела не имеется»[1].

Можно, однако, найти многочисленные примеры применения ст. 272 УК РФ при оценке действий, связанных с неправомерным доступом к общедоступной информации, хранящейся в сети «Интернет».

Так, С., прекратив свою трудовую деятельность в организации, в которой занимал должность генерального директора, и утратив в связи с этим право доступа к учетной записи администратора сайта, принадлежащего организации и используемого в деловых и маркетинговых целях, испытывая неприязненное отношение к руководству, желая опорочить деловую репутацию Общества, умышленно уничтожил и модифицировал часть компьютерной информации: изменил изображение слайдера, удалив исходные изображения, но добавив другие изображения, порочащие деловую репутацию Общества, удалил контактный телефон и сведения об имеющихся сертификатах, изменил сведения о производстве и качестве сырья, удалил информацию о партнерах, экологической безопасности продукции и т. д.[2]

Принимая подобные решения, суды, как правило, ссылаются на то обстоятельство, что виновное лицо осуществило неправомерное уничтожение, модификацию или блокирование общедоступной информации, охраняемой Федеральным законом № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации».

Согласно ст. 16 данного закона защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: 1) обеспечение за-

---

[1] Апелляционный приговор Судебной коллегии по уголовным делам Верховного суда Чувашской Республики от 3 июня 2015 г. по делу № 22-1054/2015.

[2] Приговор Октябрьского районного суда г. Архангельска от 14 декабря 2015 г. по делу № 1-352/2015.

щиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации. При этом в соответствии с ч. 3 ст. 6 указанного закона обладатель информации, если иное не предусмотрено федеральными законами, вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.

Нельзя не отметить, что данные положения в целом корреспондируют Рекомендациям по стандартизации, разработанным Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Гостехкомиссии России, определяющим безопасность информации как состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность[1].

Общедоступная информация отнюдь не является информацией, лишенной защиты. Положения об обязательном характере технологической и программной защиты общедоступной информации, размещаемой в сети «Интернет», содержатся во многих подзаконных нормативно-правовых актах. Так, в соответствии с Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 27 июня 2013 г. «Об утверждении требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами и местного самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования»[2] общедоступная информация, размещаемая на сайте в форме открытых данных, должна быть защищена от уничтожения, модификации, блокирования, а также от иных неправомерных действий в отношении такой информации. Аналогичное требование предусмотрено постановлением Правительства Российской Федерации от 10 июля 2013 г. № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации»[3].

Таким образом, положения ст. 6 и ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в своей взаимосвязи позволяют сделать вывод о том, что по смыслу ст. 272 УК РФ к «охраняемой законом информации» следует относить не только информацию ограниченного доступа, но и общедоступную информацию, в отношении которой ее обладателем приняты меры по защите от несанкционированного уничтожения, модификации или блокирования.

Объективная сторона преступления выражается в неправомерном (противоречащем закону или иному нормативному акту) доступе к компьютерной информации. Способы неправомерного доступа к компьютерной информации могут быть самыми разнооб-

---

[1] Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст).

[2] Российская газета. – 2013. – № 187 (23 авг.).

[3] Собрание законодательства Российской Федерации. – 2013. – № 29, ст. 3964.

разными (от высокотехнологичных до примитивно-бытовых) и, как правило, не влияют на юридическую оценку поведения виновного лица.

Состав преступления материальный. Преступление считается оконченным с момента наступления хотя бы одного из альтернативно перечисленных в диспозиции ч. 1 ст. 272 УК РФ последствий: уничтожения, блокирования, модификации либо копирования компьютерной информации.

Обязательным признаком объективной стороны преступления является причинная связь между действиями лица, заключающимися в неправомерном доступе к компьютерной информации, и наступившими вредными последствиями, прямо указанными в диспозиции статьи.

Уничтожение компьютерной информации может быть, как полным, так и частичным. При этом, на наш взгляд, удаление и уничтожение не являются тождественными понятиями. Как справедливо отмечает А. Ю. Чупрова, удаление информации следует рассматривать как ее сокрытие от посторонних, при котором применение специальных методов позволяет эти данные восстановить. При уничтожении информация восстановлению не подлежит[1].

Блокирование представляет собой прекращение доступа к информации для лиц, которые имеют право на такой доступ. Закрытие доступа к информационным ресурсам (блокирование), как правило, наступает в результате изменения так называемых сетевых идентификаторов пользователя – логина и пароля.

Модификация – переработка первоначальной информации, включающая в себя любые изменения, не меняющие сущности объекта. Например, реструктурирование или реорганизация базы данных, удаление или добавление записей, содержащихся в файлах и т. д. В. В. Хилюта, например, определяет модификацию компьютерной информации как внесение любых изменений, которые создадут отличие от ранее хранившейся в компьютерной сети информации (в системе или на машинном носителе собственника информационного ресурса), в результате чего потерпевшему будет причинен имущественный ущерб, а виновное лицо извлечет из этого выгоду[2].

Копирование – перенос информации или части информации с одного носителя на другой. Например, запись информации в память другого компьютера, флеш-карты и т. д.

Требует пояснения позиция, согласно которой, если в силу настроек компьютерной программы при работе с ней, пусть даже и в результате неправомерного доступа, автоматически создается резервная копия компьютерной информации, то данное действие не будет иметь уголовно-правовых последствий, поскольку оно осуществляется независимо от волеизъявления лица и, соответственно, в прямой причинной связи с его действиями не состоит[3].

---

[1] Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. – 2015. – № 5. – С. 133.

[2] Хилюта В. В. Вопросы квалификации преступлений против собственности, не являющихся хищением : монография. Минск, 2013. С. 33.

[3] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». URL: http://www.consultant.ru

В такой ситуации имеется причинно-следственная связь между действиями лица и наступившими общественно опасными последствиями в виде копирования охраняемой законом компьютерной информации.

С другой стороны, неосведомленность лица об особенностях настроек программы фактически исключает вину по отношению к копированию информации. На наш взгляд, именно по этой причине и следует утверждать об отсутствии уголовно-правовых последствий за содеянное.

Следует отметить, что в правоприменительной практике случаи использования скимминговогo оборудования[1] также квалифицируются по ст. 272 УК РФ.

Так, например, Б. совершил неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, повлекшее копирование информации, из корыстной заинтересованности, при следующих обстоятельствах. Б. приобрел в неустановленном следствием месте унеустановленного лица скимминговое оборудование в виде накладки на кардридер банкомата для тайного несанкционированного считывания информации с банковских карт, представляющего из себя радиоэлектронные сборки, смонтированные на печатных платах. Среди радиоэлектронных компонентов на платах имеются магнитная головка (магнитный сенсор), источник питания и слот для карты памяти формата MicroSD с установленной картой памяти Trancend.

После этого, Б., действуя умышленно, с целью неправомерного доступа к охраняемой законом компьютерной информации с помощью скимминговогo устройства, прибыл к месту расположения банкомата, действуя тайно от окружающих, установил скимминговое устройство на кардридер банкомата, включив при этом внутреннее питание устройства для его запуска.

В результате функционирования скрытно установленного на банкомате скимминговогo оборудования, Б. незаконным способом скопировал информацию о реквизитах 31 банковской карты, а именно: информацию о банковских счетах, на которых на момент проведения последних операций законными держателями банковских карт в указанном банкомате находились денежные средства на общую сумму 159 724, 22 руб.

При таких обстоятельствах Б., действуя умышленно, не обладая правами на доступ и работу с информацией, осуществил неправомерный доступ к компьютерной информации, охраняемой ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», вводимой в электронно-вычислительную машину банкомата законным держателем банковской

[1] Скимминг (от англ. «skim»), скимер – мошенничество с платежными картами, кардинг (от англ. «carding») – вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная и не подтвержденная держателям. Реквизиты платежных карт берут со взломанных серверов интернет-магазинов, платежных или расчетных систем, персональных компьютеров (с помощью программ удаленного доступа, «троянов», ботов). Сегодня наиболее распространенным методом похищения номеров является фишинг (англ. phishing, искаж. «fishing» – «рыбалка») – это создание мошенниками сайта, который будет пользоваться доверием у пользователя, например, сайт, похожий на сайт банка пользователя, через который происходит похищение реквизитов платежных карт.

карты при наборе на клавиатуре ПИН-кода для доступа к своему банковскому счету, что повлекло несанкционированное копирование информации, выразившееся в переносе в память скимминогового оборудования, установленного последним на кардридер банкомата, информации о реквизитах банковских карт, необходимых для проведения операций в банкомате, их обработки в процессинговом центре банка-эквайрера, серверах платежной системы, процессинговом центре банка-эмитента через систему дистанционного банковского обслуживания, в результате чего неправомерно осуществил копирование конфиденциальной клиентской информации[1].

Субъектом основного состава преступления является физическое, вменяемое лицо, достигшее шестнадцатилетнего возраста и не наделенное в силу характера выполняемой работы полномочиями доступа к компьютерной информации.

Несмотря на то, что диспозиция рассматриваемой статьи не дает прямых указаний относительно субъективной стороны преступления, можно с уверенностью говорить об умышленной форме вины в виде прямого или косвенного умысла.

В связи с этим представляется дискуссионным мнение, что субъективная сторона рассматриваемого преступления характеризуется виной в форме умысла (прямого или косвенного) или неосторожности[2].

Мотивы и цели неправомерного доступа к компьютерной информации могут быть весьма разнообразными. Анализируемое преступление может совершаться из мести, зависти, хулиганства, «спортивного интереса», желания подорвать деловую репутацию конкурента и т. д. Обязательными признаками состава преступления они не являются и, следовательно, решающего значения для квалификации не имеют. Между тем их точное установление позволит не только выявить причины, побудившие лицо совершить подобное преступление, но и назначить ему справедливое наказание.

К квалифицирующим признакам, названным в ч. 2 ст. 272 УК РФ, относится совершение данного преступления с причинением крупного ущерба или из корыстной заинтересованности.

В соответствии с примечанием к ст. 272 УК РФ ущерб признается крупным, если его сумма превышает миллион руб. С качественной стороны ущерб может выражаться как в прямых имущественных потерях обладателя информации (например, расходы, связанные с восстановлением уничтоженного или модифицированного программного обеспечения), так и в упущенной выгоде (например, недополученная прибыль в результате дезорганизации производственного процесса конкретного предприятия).

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

---

[1] Обвинительное заключение по уголовному делу № 1146014 // Архив СЧ СУ МВД по Республике Адыгея.

[2] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». URL: http://www.consultant.ru.

Так, например, Белоусов в процессе использования персонального компьютера, подключенного к сети «Интернет», обнаружил возможность неправомерного и бесплатного подключения к сети «Интернет», путем использования программы LanScope для электронно-вычислительной машины и завладения сетевыми реквизитами доступа к сети «Интернет», принадлежащих иным абонентам.

После чего Белоусов, обладая полученными знаниями о возможности неправомерного и бесплатного осуществления подключения к сети «Интернет», не желая осуществлять подключение к сети «Интернет» законным способом, а именно с использованием сетевых реквизитов, принадлежащих его родному брату, вызванного значительными затратами денежных средств на лицевом счете, нуждаясь в использовании ресурсов сети «Интернет», путем подбора цифровых значений с использованием программы для сканирования компьютерных сетей LanScope, получил сведения о сетевых реквизитах доступа к сети «Интернет» абонента краевого государственного бюджетного учреждения «Корякский фольклорный ансамбль танца «Ангт» в виде «poe-4154332248» и пароля «858630», с целью последующего их использования и обеспечения себе бесплатного доступа к сети «Интернет».

Реализуя возникший преступный умысел, Белоусов из корыстной заинтересованности, с целью обеспечения себе бесплатного доступа к сети «Интернет», при помощи персонального компьютера, подключенного к сети «Интернет» посредством оператора связи, осознавая, что имеющийся логин и пароль принадлежат действующему абоненту, предвидя возможность наступления общественно-опасных последствий в виде искажения (модификации) информации в базе учетно-статистических данных, а также возможность блокирования доступа к компьютерной информации законного пользователя логина и пароля, используя сетевые реквизиты доступа к сети «Интернет» – логин «poe-4154332248» и пароль доступа «858630», осуществил неправомерное подключение и работу в сети «Интернет» в указанный период времени со следующими параметрами сетевого соединения

Таким образом, Белоусов из корыстной заинтересованности, осуществил неправомерный (несанкционированный) доступ к охраняемой Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» компьютерной информации, а именно: информации о сетевых реквизитах КГБУ «Ангт», что повлекло искажение (модификацию) информации в базе учетно-статистических данных, а именно: информации о времени начала, продолжительности и стоимости работы в сети «Интернет» абонента КГБУ «Ангт», а также блокирование доступа к компьютерной информации, выразившееся в невозможности подключения сотрудников КГБУ «Ангт» к сети «Интернет» в указанное время и использовании предоставленного указанному учреждению внешнего трафика по технологии DSL в объеме 1 089, 51 Mb стоимостью 1 699 руб. 63 коп.[1].

[1] Обвинительное заключение по уголовному делу № 423731 // Архив СО Корякского МО МВД России.

Корыстным следует также признавать неправомерный доступ к охраняемой законом компьютерной информации, совершенный лицом по найму, то есть за вознаграждение.

Так, например, сотрудниками управления «К» МВД России была пресечена деятельность организованной группы, которая специализировалась на взломе аккаунтов в различных соцсетях, почтовых серверах и web-сайтах, организации DDOS-атак. Необходимые для этих целей программы создавали как программисты из круга общения злоумышленников, так и случайные знакомые, встреченные на специализированных сайтах. За предоставление соответствующих сведений злоумышленники получали вознаграждение[1].

Часть 3 ст. 272 УК РФ предусматривает три особо квалифицирующих признака. Неправомерный доступ к охраняемой законом компьютерной информации, совершенный: группой лиц по предварительному сговору; организованной группой; лицом с использованием своего служебного положения.

Неправомерный доступ к компьютерной информации признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении этого преступления. Принципиальным следует считать положение о том, что каждый из образующих указанную группу лиц преступников должен сыграть роль соисполнителя. При наличии одного исполнителя и отсутствии иных квалифицирующих признаков этого преступления действия остальных его соучастников необходимо оценивать по ч. 1 ст. 272 УК РФ и соответствующей части ст. 33 УК РФ[2].

Неправомерный доступ к компьютерной информации признается совершенным организованной группой, если он совершен устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Использование своего служебного положения предполагает доступ к охраняемой законом компьютерной информации благодаря занимаемому виновным положению по службе. Этот признак будет наличествовать и тогда, когда действия лица хотя и находились в пределах его служебной компетенции, но совершались с явным нарушением порядка осуществления своих функциональных обязанностей, установленных законом или иным нормативным актом. В судебно-следственной практике подобного рода действия оцениваются по-разному.

В некоторых случаях содеянное квалифицируется исключительно по ст. 285 УК РФ со ссылкой на то обстоятельство, что лицо в соответствии с занимаемой должностью имело право доступа к информационным базам с присвоением соответствующих логина и пароля.

---

[1] Задержаны хакеры, взламывавшие по заказам страницы в соцсетях, почтовые ящики и занимавшиеся прослушкой // URL: https://мвд.рф/news/show_102385 (дата обращения: 26.08.2019).

[2] Как известно, данная позиция неоднократно подтверждалась в решениях Верховного Суда Российской Федерации, напр.: Постановление Президиума Верховного Суда Российской Федерации от 25 декабря 1996 г. № 436п96 по делу В. П. Ткаченко и В. В. Хоперского // Бюллетень Верховного Суда Российской Федерации. – 1997. – № 4 ; Постановление Президиума Верховного Суда Российской Федерации от 20 августа 2003 г. № 495п03 по делу С. И. Бычкало и др. // Бюллетень Верховного Суда Российской Федерации. – 2004. – № 3.

Так, отмечается, что «…действия виновного по внесению заведомо ложных сведений об уплате штрафа, несоответствующих действительности, непосредственно связаны с осуществлением им своих прав и обязанностей, которые не вызывались служебной необходимостью и объективно противоречили как общим задачам и требованиям, предъявляемым к государственному аппарату, так и тем целям, и задачам, для достижения которых виновный, как должностное лицо было наделено соответствующими должностными полномочиями»[1].

Однако использование должностным лицом своих служебных полномочий отнюдь не исключает признания доступа к компьютерной информации неправомерным. Это объясняется тем, что право должностного лица на доступ к информационной базе данных носит не общий характер, а возникает только в связи со строго определенными (нормативно регламентированными) основаниями[2].

Так, в другом решении суд, применив ч. 3 ст. 272 УК РФ, обоснованно указал, что наличие у виновного официального доступа к служебной базе данных само по себе не исключает возможности его осуждения по ст. 272 УК РФ, поскольку им совершены незаконные действия, связанные с неправомерным доступом к компьютерной информации, имевшие целью сокрытие ранее совершенного должностного преступления, а также направленные на избежание лицом, совершившим административное правонарушение, исполнения назначенного судебным решением наказания[3].

Учитывая, что ч. 3 ст. 272 УК РФ точнее выражает направленность деяния, а также более полно описывает его признаки, следует, пожалуй, поддержать последний подход. При этом, полагаем, в силу ч. 1 ст. 17 УК РФ подобного рода действия должностных лиц полностью охватываются ч. 3 ст. 272 УК РФ и дополнительной квалификации по ст. 285 УК РФ не требуют. Исключением могут выступать лишь случаи, когда должностное лицо, используя свои служебные полномочия, наряду с неправомерным доступом к компьютерной информации, совершило другие незаконные действия, связанные со злоупотреблением должностными полномочиями из корыстной или иной личной заинтересованности. При таких обстоятельствах содеянное надлежит квалифицировать по совокупности указанных преступлений.

---

[1] Приговор Первомайского суда г. Кирова от 9 сентября 2016 г. по делу № 1-222/2016.

[2] Так, например, приказом МВД России от 3 декабря 2007 г. № 1 144 «О системе информационного обеспечения Госавтоинспекции» утверждены «Наставления по организации формирования и ведения специализированных учетов федеральной специализированной территориально распределенной информационной системы Госавтоинспекции». В соответствии с п. 2.4 указанных наставлений специализированный федеральный учет лиц, привлеченных к административной ответственности за нарушения правил дорожного движения (АИПС «Адмпрактика»), формируется на основе сведений, поступающих из подразделений Госавтоинспекции органов внутренних дел в районах, городах и иных муниципальных образованиях. Основанием для постановки на региональный учет является оформление соответствующего протокола об административных правонарушениях в области обеспечения безопасности дорожного движения (п. 9.1).

[3] Приговор Катайского районного суда Курганской области от 18 апреля 2013 г. по делу № 1-20/2013.

Несмотря на то что информация, содержащаяся в информационных базах данных, используется государственными органами при составлении официальных документов, внесение в них заведомо ложных сведений, на наш взгляд, нельзя квалифицировать как служебный подлог.

Так, в одном случае, оценив внесение инспектором дорожно-патрульной службы заведомо ложных сведений об уплате лицом административных штрафов по ч. 3 ст. 272 УК РФ, суд обоснованно не согласился с необходимостью дополнительного вменения ст. 292 УК РФ. Аргументация принятого решения основывалась на том, что «…в качестве предмета данного преступления действующим законодательством признаются лишь официальные документы. В силу требований закона официальный документ должен быть публичным, адресованным неопределенному кругу субъектов правоотношений, иметь соответствующие реквизиты и удостоверять факты, влекущие юридические последствия в виде предоставления или лишения прав, возложения или освобождения от обязанностей, изменения объема прав и обязанностей. Вопреки доводам стороны обвинения, автоматизированная информационно-поисковая система данными признаками не обладает, является базой данных для внутреннего пользования органов полиции, тем самым у суда отсутствуют основания утверждать, что Г., модифицировав компьютерную информацию в отношении Д., внесла и заведомо ложные сведения в официальный документ, совершив служебный подлог»[1].

Криминалистами проблемам электронного официального документа уделяется большое внимание[2], что объясняется прикладной значимостью соответствующих вопросов. Не углубляясь в известную полемику относительно признаков электронного официального документа как предмета преступления, отметим, что в силу положений ст. 2 Федерального закона № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» информационные системы (информационно-поисковые системы, информационные базы данных и т. п.) следует предельно четко отграничивать от электронных документов, в том числе официальных. Информационная система предназначена для накопления и обработки информации. При этом официальные электронные документы могут составлять содержание информационной системы, быть ее частью. Совокупность преступлений, предусмотренных ч. 3 ст. 272 УК РФ и ст. 292 УК РФ, может иметь место в том случае, если неправомерный доступ к компьютерной информации был сопряжен с внесением соответствующим субъектом заведомо ложных сведений в электронные официальные документы.

---

[1] Приговор Богдановичского городского суда Свердловской области от 27 августа 2015 г. по делу № 1-30/2015.

[2] Букалерова Л. А., Шагиева Р. В. О необходимости усиления правовой охраны оборота электронной подписи : современные проблемы теории и практики // Ученые труды Российской академии адвокатуры и нотариата. – 2011. – № 2 (21). – С. 119–124 ; Ефремова М. А. Электронный документ как предмет преступления // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2015. – № 5. – С. 10–15 ; Иванова Е. В. Официальный документ в электронной форме как предмет преступления, предусмотренного ст. 327 УК РФ // Уголовное право. – 2012. – № 3. – С. 29–31 ; Лукьянова А. А. Электронный официальный документ как предмет преступления, предусмотренного ст. 327 УК РФ // Уголовное право. – 2016. – № 3. – С. 57–62.

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

Понятие «тяжкие последствия» является оценочным. На практике к ним относят: причинение смерти или тяжкого вреда здоровью человека; причинение средней тяжести вреда здоровью двум или более лицам; массовое причинение легкого вреда здоровью людей; наступление экологических катастроф, транспортных или производственных аварий, повлекших длительную остановку транспорта или производственного процесса; дезорганизацию работы конкретного предприятия; причинение особо крупного ущерба и т. п.

Следует отметить, что преступление, предусмотренное ч. 4 ст. 272 УК РФ, будет иметь место не только при фактическом наступлении тяжких последствий, но и при создании угрозы их наступления. При этом угроза наступления тяжких последствий будет считаться созданной, если она была реальной, и тяжкие последствия не наступили, лишь вследствие обстоятельств, не зависящих от воли виновного, или благодаря вовремя принятым мерам.

Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)

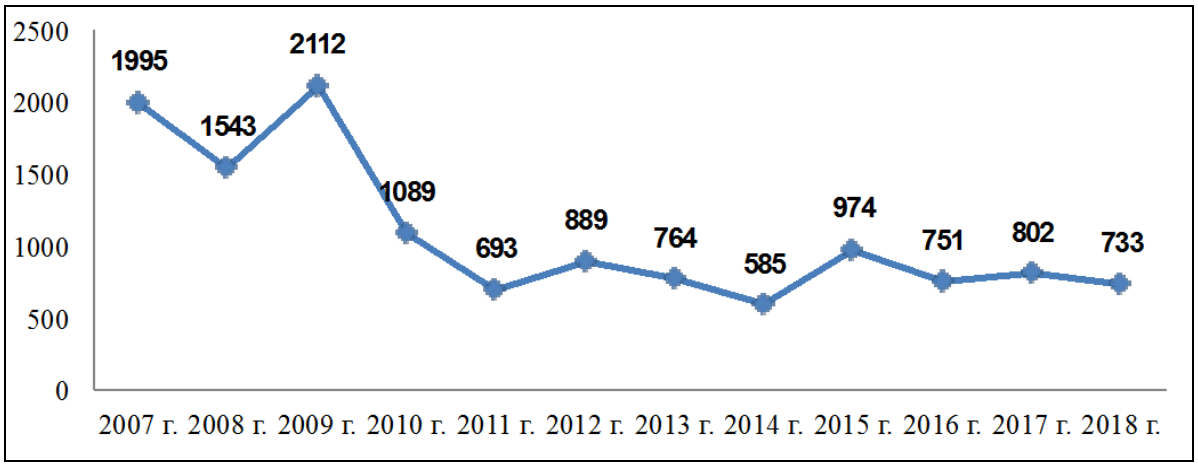

Рис. 1.3. Количество зарегистрированных преступлений по ст. 273 УК РФ

В наше время, пожалуй, трудно найти пользователя современными информационно-коммуникационными технологиями, который хотя бы раз не испытывал на себе негативное воздействие вредоносных компьютерных программ. Некоторые из них относительно безобидны, другие могут причинить непоправимый вред не только информационным активам, но и самому компьютерному оборудованию. В отношении наиболее опасных авторы предлагают и вовсе использовать термины «информационное оружие» или «кибероружие»[1].

Совсем недавние атаки на информационную инфраструктуру ряда государств, в том числе России, вирусов-шифровальщиков WannaCry и Petya не позволяют признавать такие оценки надуманными либо преувеличенными. В общей сложности только от WannaCry пострадало более 500 тыс. компьютеров, принадлежащих частным ли-

[1] Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации : учебное пособие. М., 2001. С. 40.

цам, коммерческим организациям и правительственным учреждениям, в более чем 150 странах мира[1].

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

Парадоксально, но несмотря на значимость проблемы противодействия деструктивным информационным объектам, в отечественной уголовно-правовой науке так и не сложилось единообразного понимания «вредоносной программы» как конструктивного признака ст. 273 УК РФ (рис. 1.3).

Соглашение о сотрудничестве государств–участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации определяет вредоносную программу как созданную или существующую программу со специально внесенными изменениями, заведомо приводящую к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети[2].

В этом же ключе содержание вредоносной программы раскрывается в п. 2.6.5 и 2.6.6 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», утвержденного Приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст[3]. Согласно государственному стандарту, вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Подобный подход, определяющий вредоносность программы ее функциональным предназначением – оказывать неправомерное (несанкционированное) воздействие исключительно на компьютерные данные и системы – является наиболее распространенным и в доктрине уголовного права. По мнению В. Б. Вехова, для того, чтобы признать компьютерную программу вредоносной, необходимо доказать наличие совокупности следующих обстоятельств:

– программа способна уничтожать, блокировать, модифицировать либо копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации;

– программа не предполагает предварительного уведомления собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети о характере своих действий;

---

[1] Владимир Путин назвал спецслужбы США источником вируса WannaCry. URL: http://www.kommersant.ru/doc/3297338 (дата обращения: 20.11.2019).

[2] Собрание законодательства Российской Федерации. – 2009. – № 13, ст. 1460.

[3] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М. : Стандартинформ, 2008.

– программа не запрашивает согласия (санкции) у собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети на реализацию своего назначения (алгоритма)[1].

В судебно-следственной практике, пожалуй, наибольшее распространение получило признание вредоносными компьютерных программ, которые заведомо предназначены для генерации кода установки (серийного номера) и кода активации, запрашиваемых при установке лицензионных программных продуктов («KEYGEN.exe» и др.).

Так, Розов был осужден по ч. 2 ст. 146 УК РФ и ч. 1 ст. 273 УК РФ. Согласно приговору суда Розов, находясь в помещении общества с ограниченной ответственностью, из корыстной заинтересованности выполнил несанкционированное копирование (установку) с неустановленного следствием носителя информации программного продукта «AutoCAD-2014» на системный блок электронно-вычислительной машины, принадлежащей организации и для достижения работоспособности указанного программного продукта незаконно использовал вредоносную компьютерную программу «X-Force» с неустановленного следствием носителя информации. Таким образом Розов умышленно использовал вредоносную программу «X-Force», чем заведомо исключил возможность штатной установки лицензионного ключа программы «AutoCAD-2014», и тем самым заведомо несанкционированно модифицировал (изменил) продукцию «AutoCAD-2014», обеспечив нейтрализацию средств защиты и нормальное функционирование работы программного продукта «AutoCAD-2014» неправомерно копированного (установленного) им с неустановленного следствием носителя[2].

Сравнительно реже правоохранительные органы выявляют случаи использования «компьютерных вирусов», «троянов» и т. п.

Так, например, Маликов был осужден по ч. 1 ст. 273 УК РФ. В соответствии с приговором суда Маликов, обладая специальными познаниями в области работы с компьютерными программами, действуя умышленно, находясь по месту жительства приобрел путем копирования с неустановленных интернет-ресурсов, компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации, после чего посредством принадлежащего ему компьютерного оборудования, а также находящихся в его пользовании хостинговых сервисов (серверов для хранения информации в сети «Интернет») использовал указанные вредоносные компьютерные программы для заражения 50 компьютеров неустановленных пользователей сети «Интернет» и построения из них контролируемой сети, в результате чего без ведома и согласия указанных пользователей скопировал хранящуюся в памяти зараженных устройств компьютерную информацию, содержащую сведения о логинах и паролях авторизации пользователей на различных интернет-ресурсах, которую планировал использовать в личных целях. Согласно заключению эксперта, на жестком диске персонального ком-

---

[1] Вехов В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. – 2015. – № 2 (8). – С. 45.

[2] Приговор Александровского городского суда Владимирской области от 19 августа 2015 г. по делу № 1-82/2015.

пьютера Маликова обнаружены комплексы вредоносного программного обеспечения, предназначенного для построения «ботнетов» («бот-сетей»), то есть сетей из зараженных соответствующим вирусом компьютеров с возможностью уделенного копирования информации назначенным владельцем указанной сети без ведома пользователя и без получения его согласия на применение указанных программ. Работа обнаруженного на жестком диске вредоносного программного обеспечения построена на использовании вирусов типа «троян» («троянская программа»)[1].

Господствующее толкование вредоносности компьютерной программы, к сожалению, имеет свои изъяны. Так, например, оно не позволяет отнести к таковым программы–шпионы (Spyware), целью которых является не причинение вреда информационным активам или инфраструктуре, а собирание сведений об активности пользователя в сети «Интернет» (о посещаемых сайтах, совершаемых покупках и т. п.), программы «злые шутки» (bad jokes)[2], так называемые «вирусные конструкторы» – программы, предназначенные не для осуществления атак на компьютерные ресурсы, а для генерирования новых вирусов. При общепринятом подходе нельзя отнести к вредоносным также программы, объективно приспособленные к совершению преступлений, но выполненные на основе легального программного обеспечения. В связи с этим обоснованно возникает вопрос, может ли вредоносность программы выражаться в ее направленности на совершение посягательств в отношении иных охраняемых уголовным законом объектов? В. С. Комиссаров дает утвердительный ответ на этот вопрос, поскольку считает, что вредоносность может быть обусловлена не только самим алгоритмом ее действия, направленным на уничтожение, блокирование, модификацию или копирование информации, но и «специфическими свойствами, предназначенными для выполнения неправомерных или даже преступных действий (хищения денег с банковских счетов, укрытия средств от налогообложения, хулиганства и т. д.)»[3].

В. А. Голуб и М. В. Овчинникова также расширительно толкуют содержание вредоносной программы, определяя ее как программу или фрагмент кода, специально созданную для выполнения или способствующую выполнению несанкционированных действий в информационной системе или информационно-телекоммуникационной сети, в результате которых возможно причинение вреда пользователям этой системы (сети) или другим лицам[4].

---

[1] Приговор Андроповского районного суда Ставропольского края от 6 апреля 2017 г. по делу № 1-31/2017.

[2] Такие программы не причиняют компьютеру прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен, предупреждают пользователя об опасности, которой на самом деле не существует. К «злым шуткам» относятся, например, программы, которые пугают пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), выводят сообщения, характерные для вирусов. К данному классу также можно отнести программы, которые осуществляют мошенничество путем распространения архивов с оплатой за СМС // URL: https://threats.kaspersky.com/ru/threat/Hoax.JS.BadJoke/ (дата обращения: 22.11.2017).

[3] Уголовное право: Особенная часть / под ред. А. И. Рарога. М., 2009. С. 532–533.

[4] Голуб В. А., Овчинникова М. В. Проблема корректного определения термина «вредоносная программа» // Вестник Воронежского государственного университета. – Серия: Системный анализ и информационные технологии. – 2008. – № 1. – С. 141.

Пункт 2 «Правил оказания телематических услуг связи», утвержденных постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575, вредоносное программное обеспечение раскрывает как целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя, либо к ухудшению параметров функционирования абонентского терминала или сети связи[1].

Если исходить из подобного, более широкого, понимания вредоносности как предназначения программы к заведомо противоправной (преступной) деятельности в целом, то изготовление и распространение программ-шпионов и конструкторов вирусов может быть квалифицировано по ст. 273 УК РФ. На наш взгляд, современный процесс непрерывного роста использования информационно-коммуникационных технологий во всех сферах жизни общества («виртуализация» жизнедеятельности»[2]), убедительно свидетельствует в пользу именно этого подхода. С течением времени вредоносные программные продукты все больше будут направлены не на отношения информационной безопасности как таковые, а на иные социально значимые сферы – жизнь, здоровье, честь и достоинство личности, неприкосновенность частной жизни, отношения собственности, общественный порядок и др.

К. Н. Евдокимов делает вывод, что вредоносными программами могут быть и обычные лицензионные компьютерные программы в случае их использования при совершении преступного деяния и достижения вредных последствий, указанных в ст. 273 УК РФ[3]. Полагаем, что автор необоснованно смешивает вредоносные программы и легальное программное обеспечение, которое достаточно часто используется при совершении посягательств на объекты уголовно-правовой охраны. Известно, что многие разрешенные к обороту программные продукты применяются злоумышленниками для совершения преступлений. Так, например, программы для записи дисков (InfraRecoder, BurnAware, Nero и т. д.) используются злоумышленниками для изготовления контрафактной продукции (неправомерного копирования информации), программное обеспечение для удаленного администрирования (RDP, VNC, DameWare, TeamViewer, Remote Office Manager, Hamachi, и т. д.) довольно часто применяется при совершении хищений, связанных с неправомерным вмешательством в системы дистанционного банковского обслуживания. Вместе с тем вредоносными их признавать нельзя, поскольку такие программы по факту остаются аутентичными, сохраняют стандартный набор настроек и возможностей, заложенный разработчиком.

Другое дело, когда центральную часть легальной программы (так называемый «движок») приспосабливают для совершения конкретных преступлений. Например, для незаконного пополнения баланса проездных билетов злоумышленник использует одну из многих компьютерных программ, предназначенных для записи информации с одного носителя на другой, но меняет ее интерфейс таким образом, чтобы можно было

---

[1] Собрание законодательства Российской Федерации. – 2007. – № 38, ст. 4552.

[2] Гилинский Я. И. Криминологические основы уголовного права в эпоху постмодерна // Криминологические основы уголовного права // Материалы X Российского конгресса уголовного права, состоявшегося 26–27 мая 2016 г. / отв. ред. В. С. Комиссаров. М. : Юрлитинформ, 2016. С. 296.

[3] Евдокимов К. Н. Создание, использование и распространение вредоносных компьютерных программ : уголовно-правовые и криминологические аспекты : монография. Иркутск, 2013. С. 60.

выбрать перевозчика, количество поездок, срок действия и т. п. В этом случае, на наш взгляд, можно говорить о наличии признаков изготовления вредоносной компьютерной программы, поскольку в окончательном виде полученное программное обеспечение обладает уже другими характеристиками, напрямую указывающими на ее предназначение для осуществления противоправной деятельности.

Следует упомянуть об общепринятом в доктрине уголовного права положении – вредоносность программного обеспечения категория юридическая и находится в компетенции правоприменителя. Программно-техническая экспертиза должна решать свои задачи – раскрыть общий алгоритм и особенности действия программы, предоставить значимую для следствия информацию о ее работе и т. п. Так или иначе выводы эксперта будут иметь лишь ориентирующий характер в разрешении вопроса о вредоносности программы. В свете современных угроз стремительно «виртуализующегося» общества полагаем, что единственно верным будет избрать в качестве основного критерия вредоносности программы ее изначальное и основное предназначение – осуществление противоправной деятельности. В какой сфере такая деятельность будет осуществляться, будет ли работа программы носить несанкционированный пользователем или разрешенный характер (как с конструктором вирусов) имеет второстепенное значение. Таким образом, под вредоносной следует понимать компьютерную программу, созданную (в том числе путем модификации легальной программы) для осуществления противоправной деятельности.

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

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

– использование таких компьютерных программ или такой компьютерной информации;

– распространение таких компьютерных программ или такой компьютерной информации.

Создание вредоносной программы или вредоносной компьютерной информации представляет собой целенаправленную деятельность лица, результатом которой является возникновение программного продукта с заранее заданным деструктивным функционалом. При этом необходимо отметить, что в современных условиях создание вредоносного программного обеспечения отнюдь не предполагает, что лицо обладает профессиональными навыками программирования. Созданием также будет являться получение вредоносного программного продукта в результате использования так называемых «конструкторов вирусов».

Так, например, Халатов совершил создание вредоносной компьютерной программы, заведомо приводящей к несанкционированному уничтожению информации, а равно распространение такой программы. Халатов, находясь по месту своего жительства, используя принадлежащий ему компьютер, обладая знаниями компьютерного программирования, знаниями команд и компилятора «Си», умышленно, с целью распространения машинного носителя с вредо-

*носной программой, путем написания в текстовом файле перечня команд «Си», удаляющих файлы с расширением «doc», «xls» самостоятельно создал вредоносную компьютерную программу, заведомо приводящую к несанкционированному удалению файлов с расширениями *. zip, * rar, * xls, *doc, из корневого каталога диска C:/и из всех каталогов и подкаталогов дисков D:\, E:\, F:\, G:\, H:\, I:\ компьютера, на который она была установлена и, тем самым приводящую к уничтожению информации, нарушению работы операционной системы семейства MicrosoftWindows. Указанную программу Халатов скопировал в выполняемый файл с расширением «exe» под названием «delete. exe», записав на машинный носитель; CD-R «Digitex 1 – 52 × compatible multi speed max drive CD-R 700 MB / 80 MIN» в целях дальнейшего распространения, и хранил при себе до момента, когда по заранее достигнутой предварительной договоренности с Федоровым – сотрудником ОБЭП Санкт-Петербургского ЛУВДТ, выступавшим в роли покупателя при проведении оперативно-разыскного мероприятия «Проверочная закупка», действуя умышленно, из корыстных побуждений, распространил путем продажи Федорову за 1 800 руб. указанный диск*[1].

Под использованием вредоносной программы или вредоносной компьютерной информации следует понимать их непосредственный запуск, совершение действий по включению вредоносной программы. Использование вредоносной программы может осуществляться как в автономном режиме, так и в информационно–коммуникационной сети, в том числе сети «Интернет».

Так, например, Абросов с помощью своего компьютера, подключенной к информационно-телекоммуникационной сети «Интернет» через провайдера умышленно, с целью блокирования компьютерной информации, используя вредоносную компьютерную программу «ХОИК», заведомо предназначенную для несанкционированного блокирования компьютерной информации, осуществил компьютерную атаку типа «отказ в обслуживании» на сайт, принадлежащий официальному сайту Президента Российской Федерации[2].

Использованием вредоносной компьютерной программы также является широко распространенная практика установления пользователями контрафактного программного обеспечения (без активации ключа правообладателя) с последующим запуском патч-файла, устраняющим средство защиты компьютерной информации.

Так, например, Карташов с целью обеспечения эксплуатации без ограничения по времени программного продукта Microsoft Office Professional 2007 Russian, правообладателем которого является Корпорация Microsoft Corporation, без активационного ключа правообладателя, возник умысел, направленный на использование компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации. Реализуя свой преступный умысел, Карташов, не имея соответствующего разрешения от правообладателя, произвел установку на жесткий диск компьютера один экземпляр программного продукта Microsoft Office Professional 2007 Russian. Затем Карташов во время

---

[1] Приговор Смольнинского районного суда г. Санкт-Петербург от 2 февраля 2011 г. по делу № 1-65/11.

[2] Приговор Курганского городского суда от 21 сентября 2015 г. по делу № 1-1388/15.

установки вышеуказанного программного продукта, осознавая общественную опасность своих действий, предвидя наступление общественно опасных последствий и желая их наступления, с целью активации, регистрации и приведения контрафактного программного продукта Microsoft Office Professional 2007 Russian, в работоспособное состояние и нейтрализации технических средств защиты авторского права указанного программного продукта, после нажатия клавиши запуска указанной программы, на предложение программы ввести лицензионный ключ, двойным нажатием на файл «Ключ.txt», ранее приобретенный им путем скачивания из сети «Интернет» и хранимый на USB-флеш-накопителе в каталоге «:\Microsoft Office 2007 Professional SP3 (все обновления на 01.11.2014) Russian», открыл его и скопировал указанный там ключ в предложенное для ввода окно, чем активировал вышеуказанный программный продукт. Вышеуказанные действия Карташова повлекли нейтрализацию встроенной программной защиты от несанкционированного использования программного продукта Microsoft Office Professional 2007 Russian, правообладателем которого является Корпорация Microsoft Corporation, а также снятие функциональных и временных ограничений, нейтрализацию встроенной программной защиты от несанкционированного использования, и нарушение их нормального функционирования[1].

Распространение вредоносной программы или вредоносной компьютерной информации заключается в сознательном предоставлении доступа воспроизведенной в любой материальной форме программе или информации, в том числе сетевым и иным способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей. Например, распространение таких программ может быть осуществлено при работе виновного на чужом компьютере, путем использования носителя с записью, содержащей вредоносную программу или информацию, посредством ее копирования с диска на диск.

Распространение может осуществляться и посредством информационно-телекоммуникационной сети, в том числе информационно-телекоммуникационной сети «Интернет».

Так, например, Миронов распространил компьютерные программы и иную компьютерную информацию, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации при следующих обстоятельствах.

Миронов в целях извлечения для себя личной выгоды, выраженной в получении нематериальных благ и иных преимуществ в виде безвозмездного пользования компьютерной информацией, используя свои познания в области компьютерных технологий и специальную программу для ЭВМ, путем копирования через сеть незаконно приобрел у неустановленного лица и сохранил на жестком диске своего системного блока программные продукты, содержащие две компьютерные программы, предназначенные для взлома программных продуктов, а также компьютерную информацию – один командный файл, блокирующий проверку подлинности лицензионных номеров, полученных спо-

[1] Приговор Бийского городского суда от 26 марта 2015 г. по делу № 1-250/2015.

собом генерации с помощью вышеуказанных программ, заведомо позволяющие осуществлять несанкционированное уничтожение, блокирование, модификацию, копирование, вносить изменения в существующие программные продукты и производить нейтрализацию средств защиты компьютерной информации.

После этого Миронов, имея преступный умысел, направленный на незаконное распространение вышеуказанных вредоносных компьютерных программ и компьютерной информации, используя компьютерную технику и специальную программу для ЭВМ, незаконно выложил в сеть, а именно на интернет-хабе вышеуказанные программные продукты, тем самым незаконно распространив их и предоставив неограниченному кругу пользователей данной сети возможность их копирования и использования по своему усмотрению[1].

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

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

Состав преступления, предусмотренный ч. 1 ст. 273 УК РФ, сконструирован по типу формального, что прямо вытекает из буквы и смысла закона. Следовательно, для признания преступления оконченным не требуется наступления вредных последствий в виде уничтожения, блокирования, модификации копирования информации либо нейтрализации средств защиты компьютерной информации. Достаточно установить факт совершения хотя бы одного из альтернативно перечисленных в диспозиции статьи действий.

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

Так, например, Зинченко, оказывая услуги по установке контрафактного программного обеспечения, подсоединил к системному блоку компьютера имеющийся у него USB жесткий диск WesterenDigital, на котором хранилась программа «1С Предприятие, версия 8.2», установил на жесткий диск «D» персонального компьютера файлы программы «1С Предприятие, версия

[1] Приговор Октябрьского районного суда г. Ижевска от 23 июня 2014 г. по делу № 1-186/14.

[2] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». URL: http://www.consultant.ru.

8.2». Затем для изменения конфигурации данной программы «Управление производственным предприятием» воспользовался программой «патч» предназначенной для активизации. После этого он проверил работоспособность вышеуказанной программы, запустив ее. Программа работала исправно. Он сообщил присутствовавшему при установке программы «1С Предприятие, версия 8.2» мужчине по имени Дмитрий, что программа установлена и попросил с ним рассчитаться. Дмитрий достал из кошелька денежные средства в сумме 7 200 руб. (1 купюра достоинством 5 000 руб., 2 купюры достоинством 1 000 руб. каждая, 2 купюры достоинством 100 руб. каждая) и передал их Зинченко за оказанную услугу. После чего Зинченко убрал данные денежные средства в карман своей одежды, отсоединил от персонального компьютера свой USB жесткий диск WesterenDigital и пошел к выходу из офиса, где был остановлен сотрудником полиции, который объявил, что была проведена проверочная закупка.

Зинченко является пользователем сети «Интернет» более 10 лет. Данную компьютерную программу «1С: Предприятие 8.2 Управление производственным предприятием» (дистрибутив) он скачал из сети «Интернет». Тем же способом он скачал «патч» – программу «Emul Small × 32 Setup.exe», которая предназначена для активации работы программ фирмы 1С.

Согласно заключению компьютерно-технической судебной экспертизы на переносном жестком диске WESTERNDIGITAL S/NWXE607647066 обнаружен программный продукт «1С:Предприятие 8. Управление производственным предприятием» (дистрибутив), имеет в директориях с программным продуктом файлы программ, устраняющих и (или) позволяющих обойти защиту от несанкционированного копирования и использования, что является признаком контрафактности, а лицензионный программный продукт распространяется в виде дистрибутива только на носителях, имеющих установленные правообладателем комплектацию и оформление. Правообладателем данного программного продукта является ООО «1С». Розничная стоимость программного продукта «1С: Предприятие 8. Управление производственным предприятием» (дистрибутив) составляет 155 000 руб.

На внутреннем жестком диске № Z3T4LKLP системного блока AQUARIUS персонального компьютера обнаружены контрафактные программные продукты: 1) «1С: Предприятие 8. Управление производственным предприятием» (установленные программные продукты), 2) «1С: Предприятие 8. Управление производственным предприятием» (дистрибутив), правообладателями которых является ООО «1С». Розничная стоимость каждого из двух вышеуказанных экземпляров программных продуктов составляет 155 000 руб.

На внутреннем жестком диске № Z3T4LKLP системного блока в директории C:\Users\Администратор\Desktop\1C.Predriyatie.8.2010.PC_ [bigtorrent.org]\-1C.Predriyatie.8.2010.PC\Crack\» имеется файл программы EmulSmallx32Setup.exe. Из свойств файла «дата записи» на внутренний жесткий диск № Z3T4LKLP системного блока: 29.09.2014 17:00. На переносном жестком диске WESTERNDIGITAL S/NWXE607647066 в директории «...\soft\1C.Predriyatie.8.2010.PC_[bigtorrent.org]\ 1C.Predriyatie. 8.2010.PC\Crack\» имеется файл программы EmulSmallx32Setup.exe. Из свойств файла «дата записи» на переносной жесткий диск S/NWXE607647066: 29.09.2014 10:20.

В ходе экспертного эксперимента установлено, что данная программа предназначена для «эмуляции» «аппаратного ключа» защиты программного продукта «1С: Предприятие 8.2» без ведома правообладателя – ООО «1С» (т. е. с помощью программы можно осуществить доступ к компьютерной информации, без ведома правообладателя, путем установки на ЭВМ, что позволяет осуществить работу программы без ключа аппаратной защиты, то есть нейтрализацию встроенной программно-аппаратной защиты от несанкционированного использования), что является явным признаком вредоносности данной программы.

Использование программы EmulSmallx32Setup.exe иными способами, кроме указанных выше, по мнению эксперта, невозможно[1].

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

С субъективной стороны данное преступление совершается только с прямым умыслом. Виновный осознает, что создает такую программу либо компьютерную информацию, которая способна уничтожить, заблокировать, модифицировать либо копировать информацию, нейтрализовать средства защиты компьютерной информации, либо использует или распространяет вредоносную программу и желает эти действия совершить. Прежде всего это подтверждается четким указанием закона на заведомый характер деятельности виновного. Уже один этот факт исключает возможность совершения данного преступления по неосторожности либо с косвенным умыслом.

Мотивы анализируемого преступления и его цели (а они могут быть самыми разнообразными – месть, хулиганство, эксперимент и т. д.) – не являются обязательными признаками состава и учитываются лишь при назначении наказания.

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

Часть 2 ст. 273 УК РФ в качестве квалифицирующего признака преступления предусматривает его совершение группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенное из корыстной заинтересованности.

Особо квалифицирующим признаком создания, распространения или использования компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, является совершение данных деяний, если они повлекли тяжкие последствия или создали угрозу их наступления.

---

[1] Обвинительное заключение по уголовному делу № 100995 // Архив СУ МУ МВД России «Коломенское» г. Коломна Московская область.

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

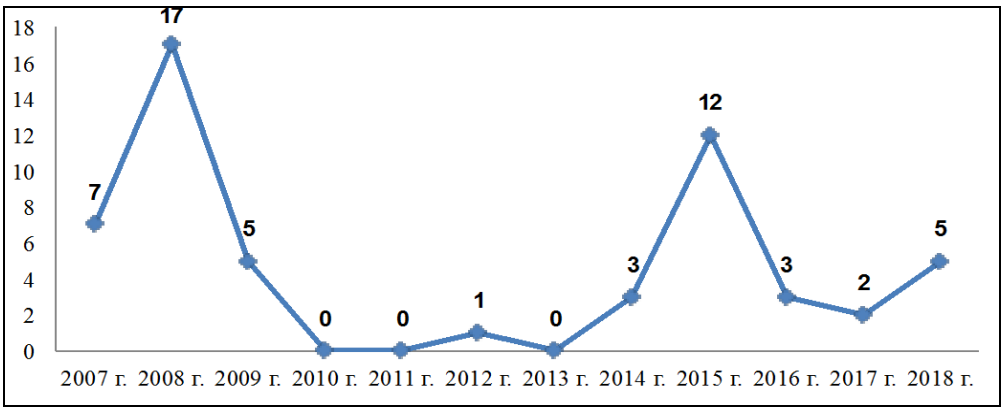

Рис. 1.4. Количество зарегистрированных преступлений по ст. 274 УК РФ

Установление уголовной ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям имеет целью предупреждение невыполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой компьютерной информации.

Объектом рассматриваемого преступления является совокупность общественных отношений в сфере соблюдения установленных правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям.

Диспозиция ст. 274 УК РФ бланкетная. Поэтому для уяснения признаков объективной стороны преступления необходимо, прежде всего, обратиться к тем конкретным положениям, закрепляющим правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правила доступа к информационно-телекоммуникационным сетям, которые были нарушены виновным. По справедливому мнению, Н. А. Лопашенко, не совсем ясно, что следует понимать под данными правилами. Имеются ли в виду технические правила обращения с компьютерной техникой (условно говоря – не бить, не ронять и т. п.), или же речь идет о правилах обращения с компьютерной информацией. Отсутствие ответов на эти вопросы, отмечает автор, расширяет сферу преступного деяния, а границы криминализации делаются сверхподвижными, их наполняют реальным содержанием правоприменители, что недопустимо, поскольку противоречит принципу законности уголовного законодательства[1].

В методических рекомендациях Генеральной прокуратуры Российской Федерации указано, что анализируемая норма является бланкетной и отсылает к конкретным инструкциям и правилам, устанавливающим порядок работы со средствами хранения,

[1]Лопашенко Н. А. Уголовно-правовая и криминологическая политика государства в области высоких технологий // URL: http://sartraccc.ru/i.php?filename=Pub%2Flopashenko%2830-06%29.htm-&oper= read_file (дата обращения: 10.01.2020).

обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием в ведомстве или организации. Эти правила должны устанавливаться правомочным лицом. Общих правил эксплуатации, распространяющихся на неограниченный круг пользователей глобальной сети «Интернет» не существует[1].

В отличие от ряда иных специальных правил, сосредоточенных в конкретных нормативных актах, правила эксплуатации средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей не консолидированы и содержатся во множестве источников. В связи с этим возникает насущная потребность по возможности четкого определения их перечня.

Прежде всего, такие правила устанавливаются на уровне нормативных правовых актов. В качестве примера можно привести постановление Правительства Российской Федерации от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи»[2], приказ Министерства связи и массовых коммуникаций Российской Федерации от 25 августа 2009 г. № 104 «Об утверждении Требований по обеспечению целостности, устойчивости, функционирования и безопасности информационных систем общего пользования»[3] и др. Последний классифицирует информационные системы общего пользования и регламентирует минимальные требования при их эксплуатации: использование сертифицированных антивирусных средств, наличие технических средств охраны помещений, в том числе систем видеонаблюдения, осуществление регистрации действий обслуживающего персонала и т. д.

В более конкретизированном виде правила пользования объектами информационно-телекоммуникационной инфраструктуры (оконечным оборудованием, терминалами оплаты, сайтами и т. п.) определяются на договорной основе (клиентским договором, договором на оказание услуг телематической связи, пользовательским соглашением и т. п.).

Так, по одному из дел суд обоснованно указал, что «…правила эксплуатации клиентом устройства самообслуживания определяется правилами пользования платежной картой, внедряемой в банкомат в ходе его эксплуатации клиентом. В свою очередь правила пользования платежной картой определяются условиями банковского договора, на основании которого клиент и получил в свое распоряжение указанную платежную карту»[4].

Самостоятельным и значимым блоком следует признать правила, разработанные и утвержденные в конкретной организации (ведомстве) при определении обязанностей работников (служащих). В настоящее время специальными положениями или должностными инструкциями конкретных сотрудников, как правило, предусмотрены определенные ограничения по использованию компьютерной техники и сети «Интернет». Типовыми правилами по эксплуатации являются запреты: загружать, самостоятельно

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». URL: http://www.consultant.ru.

[2] Собрание законодательства Российской Федерации. – 2007. – № 38, ст. 4552.

[3] Российская газета. – 2009. – № 188 (7 окт.).

[4] Приговор Кировоградского городского суда Свердловской области от 5 августа 2016 г. по делу № 1-105/2016.

устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в должностные обязанности лица; использовать интернет-ресурсы в неслужебных целях; допускать к работе посторонних лиц; подключаться к интернет-ресурсам, используя компьютерную технику компании через не служебный канал доступа – сотовый телефон, модем и другие устройства; производить какие-либо действия с информацией, зараженной вирусом и т. п.

Так, прекращая уголовное дело в отношении А. в связи с истечением сроков давности, суд отдельно указал, что подсудимый был ознакомлен с должностной инструкцией по должности ведущий системный администратор, согласно которой ведущий системный администратор поддерживает в рабочем состоянии программное обеспечение рабочих станций с серверов (п. 2.6), обеспечивает своевременное копирование, архивирование и резервирование данных (п. 2.8), обеспечивает сетевую безопасность (п. 2.18), сохраняет конфиденциальность служебной информации (п. 2.26)[1].

Бланкетные признаки ст. 274 УК РФ раскрываются и в правилах, установленных производителем компьютерного оборудования, то есть содержащихся в соответствующей технической документации. Таковыми, в частности, выступают общепринятые запреты на использование неоригинальных адаптеров переменного тока или батарей, осуществление работы в условиях перекрытия воздушного потока и др. Следует, однако, отметить, что при применении ст. 274 УК РФ необходимо установить, что лицо было ознакомлено (например, работодателем) с соответствующими техническими нормами или в силу фактических обстоятельств дела осознавало или должно было осознавать, что совершаемые им действия явно противоречат руководству по эксплуатации средств хранения, обработки ил передачи компьютерной информации.

А. Н. Ягудин делает вывод, что по смыслу ст. 274 УК РФ под «правилами эксплуатации» следует также понимать общепринятые нормы работы в сети «Интернет», направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей[2].

Полагаем, что такая позиция требует уточнения. Утверждение в общей форме о незаконности действий лица, противоправности избранного варианта поведения («в нарушение установленного порядка», «вопреки общепринятым нормам» и т. п.) без указания на источник правовой оценки и конкретизации конкретных пунктов нарушенных правил эксплуатации является недопустимым. Как справедливо пишет Н. И. Пикуров, отсутствие в постановлении о привлечении в качестве обвиняемого или в приговоре ссылки на нарушение предписаний конкретных пунктов и статей специальных правил означает незавершенность квалификации преступления[3].

---

[1] Постановление о прекращении уголовного дела Лефортовского районного суда г. Москвы от 13 января 2015 г. по делу № 1-401/2014.

[2] Ягудин А. Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей : автореф. … дис. канд. юрид. наук. М., 2013. С. 14.

[3] Пикуров Н. И. Квалификация преступлений с бланкетными признаками состава : монография. М., 2009. С. 138.

Следует отдельно отметить, что примеры повседневной небрежности, повлекшие уничтожение или повреждение компьютерного оборудования, уничтожение или модификацию данных и, как следствие, причинение имущественного ущерба потерпевшему, на наш взгляд, неправильно квалифицировать по ст. 274 УК РФ. При подобных обстоятельствах, когда лицо роняет компьютер, заливает его кофе или иным образом приводит в негодное для эксплуатации состояние, деяние не связано с нарушением специальных правил. Как представляется, содеянное не образует признаков какого-либо преступления и может выступать основанием для дисциплинарной и гражданско-правовой ответственности работника.

Объективная сторона преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, состоит из общественно опасного деяния в форме действия или бездействия, наступивших общественно опасных последствий и причинной связи между ними.

К действиям в смысле ст. 274 УК РФ можно, например, отнести: нарушение запрета на подключение служебного оборудования к сети «Интернет»; предоставление посторонним лицам доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации; несанкционированное разглашение логина или пароля законного пользователя; использование нелицензионного программного обеспечения; несанкционированная модификация программного обеспечения; несанкционированное изменение параметров настройки компьютера или информационно-телекоммуникационной сети; отключение средств противовирусной защиты и др. Преступное бездействие может проявляться в несоблюдении или прямом игнорировании соблюдения установленных правил, обеспечивающих должную работу средств хранения, обработки или передачи охраняемой компьютерной информации. Например, виновный не проверяет используемые средства хранения или передачи информации на наличие вредоносных программ, не включает систему защиты информации от несанкционированного доступа к ней, не выполняет обязательной процедуры резервного копирования компьютерной информации, оставляет без присмотра рабочее место и др.

Обязательным признаком объективной стороны этого преступления являются общественно опасные последствия. При этом необходимо отметить, что закон в ст. 274 УК РФ выделяет как бы два уровня последствий, каждый из которых является обязательным для признания состава преступления оконченным. В качестве последствий основного состава преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, является уничтожение, блокирование, модификация либо копирование охраняемой законом компьютерной информации и причинение крупного ущерба (в соответствии с примечанием к ст. 272 УК РФ ущерб, сумма которого превышает млн руб.). Таким образом, формулировка закона исключает возможность привлечения лица к уголовной ответственности по ст. 274 УК РФ, если нарушение указанных правил хотя и повлекло уничтожение, блокирование, модификацию либо копирование информации, но объективно не причинило крупного ущерба.

Субъект преступления специальный – физическое, вменяемое лицо, достигшее к моменту совершения преступления шестнадцатилетнего возраста, которое, в силу характера выполняемой трудовой, профессиональной или иной деятельности, имеет беспрепятственный доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию и на которое, в силу закона или иного нормативного акта, возложено соблюдение соответствующих правил эксплуатации или доступа.

Субъективная сторона преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям характеризуется двумя формами вины.

Нарушение правил эксплуатации и доступа, предусмотренное ч. 1 ст. 274 УК РФ, может совершаться как умышленно (при этом умысел должен быть направлен на нарушение правил эксплуатации и доступа), так и по неосторожности.

Так, например, Анисимов, имея умысел на нарушение правил эксплуатации средств хранения, передачи охраняемой компьютерной информации, повлекшее копирование компьютерной информации, находясь на своем рабочем месте, используя средства авторизации (логин и пароль), и имея, в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, и действуя в нарушение Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ, ст. 1225 ГК РФ «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации», Указа Президента Российской Федерации от 6 марта 1997 г. № 188 «Перечень сведений конфиденциального характера», соглашения о сохранении служебной и коммерческой тайны, соглашения о конфиденциальности для сотрудников, а также должностной инструкции по должности ведущий системный администратор, скопировал на USB – носитель информацию из базы данных, а именно: не менее 40 тыс. записей, содержащих непрошедших проверку имен, фамилий, никнеймов (имена, которые используется при регистрации на интернет сайтах), а так же адресов электронной почты.

После чего Анисимов передал вышеуказанную информацию А. И. В., который не был осведомлен о том, что полученная им информация охраняется действующим законодательством Российской Федерации.

Вышеуказанные действия Анисимова причинили ущерб, который выражается в следующих вынужденных действиях, которые были проведены сотрудниками юридического лица, а именно:

– восстановление доступа к базе данных после смены всех паролей сотрудников, имеющих доступ к VPN-серверам, а также смена паролей в учетных записях серверов и сервисов (общие затраты 388 000 руб.);

– проведения комплекса мероприятий, направленных на поиск лица (Анисимова), которое копировало информацию из базы данных (общие затраты 153 000 руб.);

– средний простой 115 сотрудников, имеющих доступ к VPN-серверам, из-за необходимости перенастройки VPN-серверов, составил 12 ч, т. е. суммарно 920 ч на

ожидание восстановления доступа к VPN-серверам, которые были оплачены организацией (общие затраты 414 000 руб.);

– покупка оборудования для сотрудников, взамен изъятого у Анисимова по окончании служебной проверки (общие затраты 45 330 р);

– введение дополнительных средств учета лиц, осуществляющих доступ к базе данных ООО «Приват Трэйд», а также механизмов сохранения информации, направленных на недопущение копирования информации без согласования с руководством организации (общие затраты 155 270 руб.).

Таким образом, Анисимов нарушил правила эксплуатации средств хранения и передачи охраняемой компьютерной информации, повлекшее копирование компьютерной информации, чем причинил крупный вред юридическому лицу на общую сумму 1 155 600 руб.[1].

Мотивы преступления и его цели (если таковые имеются) не являются необходимыми признаками субъективной стороны анализируемого преступления и, следовательно, на квалификацию не влияют. Однако они должны учитываться в рамках общих начал назначения наказания.

Квалифицирующим признаком нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, является совершение данного деяния, если оно повлекло тяжкие последствия или создало угрозу их наступления.

§ 1.2. Неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации

С 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. №194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и ст. 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”»[2], которым гл. 28 УК РФ была дополнена специальной нормой об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274.1).

Специальная уголовно-правовая охрана информационно-коммуникационного комплекса, обеспечивающего нормальное функционирование особо важных для общества и государства объектов, не является изобретением российского законодателя и встречается во многих современных правовых режимах. Положения об уголовной ответственности за посягательства на публичные информационные ресурсы, обладающие исключительной значимостью, имеются в законодательстве Великобритании, Германии, Китая, Сингапура, США, Франции и др. В рамках СНГ использование категории «объект критической информационной инфраструктуры» пока еще не получило широкого распространения. Так, среди квалифицирующих признаков совершения компью-

[1] Постановление Лефортовского районного суда г. Москвы от 13 января 2015 г. по делу № 1-401/2014 (дело было прекращено по основаниям, предусмотренным ст. 78 УК РФ).

[2] Российская газета. – 2017. – № 167. – 31 июля.

терных преступлений в УК Азербайджана содержится указание на «инфраструктурные объекты общественного значения». В соответствии с примечанием к ст. 271 УК Азербайджана, под такими объектами подразумеваются государственные учреждения, предприятия, организации, неправительственные организации (общественные объединения и фонды), кредитные организации, страховые компании, инвестиционные фонды, которые представляют большую значимость для государства и общества[1]. К примеру, новый УК Республики Казахстан использует ограничительный подход и дифференцирует преступления в сфере компьютерной информации в зависимости от их направленности на «государственные электронные информационные ресурсы и информационные системы государственных органов», то есть только те электронные информационные ресурсы, которые были созданы или приобретены за счет бюджетных средств[2].

Всемирно известными примерами компьютерных атак на критическую инфраструктуру государства являются остановка центрифуг иранской атомной станции с помощью компьютерного вируса StuxNet в сентябре 2010 г. и выведение из строя нескольких крупных финансовых учреждений Южной Кореи в марте 2013 г. Отечественные объекты также подвергались неправомерным воздействиям со стороны киберпреступников. При этом назначенные наказания за их совершение нельзя назвать не то чтобы строгими, но хотя бы относительно адекватными содеянному. Так, в мае 2012 г. житель Красноярска, являясь последователем движения Anonymous, совершил хакерскую атаку на сайт Президента Российской Федерации. Суд приговорил его к одному году лишения свободы. Примерно через год практически идентичную атаку совершил житель Томска, вызвав блокировку указанного сайта. По данному делу суд назначил еще более мягкое наказание – полтора года ограничения свободы[3].

Не впадая в бесплодный оптимизм, следует с сожалением констатировать, что в будущем инциденты подобного рода более чем вероятны. Меры информационной защиты, подобно всем мерам юридического противодействия криминальным явлениям, всегда имеют догоняющий характер. Стремительно развивающаяся архитектура виртуального пространства не только качественно улучшает нашу жизнь, но и параллельно с этим генерирует новые риски и угрозы. В докладе The Global Risks Report 2016, подготовленном по итогам Давосского экономического форума, среди актуальных угроз мировой экономике назван выход из строя критически важной информационной инфраструктуры (critical information infrastructure breakdown)[4]. В связи с чем информационные ресурсы стратегического значения, связанные с обеспечением общественной и государственной безопасности, должны быть действенно и эффективно защищены, в том чис-

---

[1] Уголовный кодекс Азербайджанской Республики от 30 декабря 1999 г. №787-IQ (с изм. и доп. по сост. на 31.05.2016) // URL : http://online.zakon.kz/m/Document/?docid=30420353#sub_ id=2710000 (дата обращения: 07.01.2020).

[2] Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V (с изм. и доп. по сост. на 11.07.2017) // URL : http://online.zakon.kz/m/Document/?doc_id=33885902 #sub_id=320200 (дата обращения: 07.01.2020).

[3] Осужден томский хакер, взломавший сайт Президента Российской Федерации // РИА Новости. – 2013. – 23 дек.

[4] The Global Risks Report 2016 // URL: http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/world-economic-forum-global-risk-report-2016.pdf (дата обращения: 27.01.2020).

ле с помощью системы дифференцированных мер уголовной ответственности за посягательства на их доступность и целостность.

Редакция ст. 274.1 УК РФ представляет собой объединение трех традиционных для отечественного законодательства форм преступного посягательства на безопасность компьютерных данных и систем:

– неправомерный доступ;

– создание и распространение вредоносного контента;

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации.

По смыслу ст. 274.1 УК РФ, все эти деяния должны быть направлены против объектов критической информационной инфраструктуры. Таким образом, анализируемая уголовно-правовая норма конкурирует сразу с тремя статьями (ст.ст. 272–274 УК РФ) и является специальной по отношению к ним. В некотором смысле конструирование ст. 274.1 УК РФ противоречит сложившимся отечественным традициям криминализации и использования приемов юридической техники при описании уголовно-правовых норм. Следуя им, установление более строгой уголовной ответственности за посягательства на объекты критической информационной инфраструктуры предпочтительнее было бы реализовать путем выделения соответствующих квалифицирующих и особо квалифицирующих признаков в ст.ст. 272–274 УК РФ.

Анализируемая уголовно-правовая норма имеет бланкетный характер, что предполагает обязательное обращение к Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1].

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

Предметом преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, является компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры. Нельзя не отметить, что установление данного признака на практике может вызвать значительные затруднения. Функциональная направленность вредоносной программы, то есть ее предназначение именно для посягательств на соответствующие объекты, может быть установлена только в случае уникальности средств и технологий программной защиты объектов критической информационной инфраструктуры, что представляется маловероятным.

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

[1] Российская газета. – 2017. – № 167 (31 июля).

промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности.

Относимость того или иного информационного ресурса к критическому определяется посредством его включения в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

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

– создание;

– использование;

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

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

Объективная сторона преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре. Состав по конструкции является материальным. Преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. Таким образом, следует сделать вывод, что сам по себе неправомерный доступ (так называемое «чистое хакерство», осуществляемое из профессионального интереса без намерения причинить вред) по смыслу ч. 2 ст. 274.1 УК РФ не является преступлением. В свою очередь, если лицу, осуществившему неправомерный доступ к компьютерной информации, содержащейся в критической информационной инфраструктуре, по независящим от него обстоятельствам не удалось причинить вред критической информационной инфраструктуре Российской Федерации (например, в результате успешного срабатывания антивирусного программного обеспечения или действий сотрудников, отвечающих за информационную безопасность организации) содеянное следует квалифицировать как покушение на преступление по ч. 3 ст. 30, ч. 2 ст. 274.1 УК РФ.

Вред как конструктивный признак состава преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, не конкретизирован. Системное толкование отечественного уголовного законодательства позволяет сделать вывод, что таковым является уничтожение, блокирование, модификация, копирование информации, содержащейся в критической информационной инфраструктуре, нейтрализация средств защиты указанной информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование критической информационной инфраструктуры (за исключением случаев, когда это повлекло причинение смерти или тяжкого вреда здоровью человека, причинение средней тяжести вреда здоровью двум или более лицам, массовое причинение легкого вреда здоровью людей, наступление экологических катастроф, транспортных или производственных аварий, повлекших длительную остановку транспорта или производственного процесса, дезорганизацию работы конкрет-

ного предприятия, причинение особо крупного ущерба, то есть тяжких последствий[1], предусмотренных ч. 5 ст. 274.1 УК РФ).

Следует отдельно указать, что диспозиция ч. 2 ст. 274.1 УК РФ по сути содержит признаки составного преступления, поскольку указывает, что под неправомерным доступом следует также понимать доступ с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ. Таким образом, ч. 2 ст. 274.1 УК РФ охватывает и не требует квалифицировать по совокупности, неправомерный доступ к объектам критической информационной инфраструктуры, совершенный с использованием заведомо предназначенных для этого вредоносных программ (ч. 1 ст. 274.1 УК РФ) или иных вредоносных программ (ст. 273 УК РФ). При этом, если лицо, использовавшее программу, являлось и ее разработчиком, содеянное необходимо квалифицировать по совокупности преступлений. В данном случае вполне применимо известное правило квалификации, согласно которому действия по подготовке или исполнению деяния, не входящие в объективную сторону оконченного преступления (которые, по сути, не являются юридически значимым способом совершения этого преступления), должны получить самостоятельную уголовно-правовую оценку по другой статье закона[2].

Кроме того, совокупность преступлений, предусмотренных ст. 273 УК РФ и ч. 1 ст. 30, ч. 2 ст. 274.1 УК РФ, может иметь место и в том случае, когда лицо создает компьютерную программу либо иную компьютерную информацию, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Однако в этом случае необходимо доказать умысел лица на их дальнейшее использование.

Практически значимым аспектом является оценка действий субъекта, который за вознаграждение изготавливает вредоносное программное обеспечение, предназначенное по своим характеристикам на осуществление атаки на объект критической информационной инфраструктуры, и сбывает его. При отсутствии осведомленности о том, что с данным информационным орудием собирается делать заказчик, действия соответствующих лиц нельзя признать согласованными и совместными. Это исключает саму постановку вопроса о возможности соучастия в данном случае. При обратной ситуации, когда лицо понимает, для каких целей изготавливается данная программа, содеянное необходимо квалифицировать как пособничество в совершении неправомерного доступа, то есть по ч. 5 ст. 33, ч. 2 ст. 274.1 УК РФ.

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

---

[1] Гузеева О. С. Преступления, совершаемые в российском сегменте сети «Интернет» : монография. М. : Академия Генеральной прокуратуры Российской Федерации, 2015. С. 37 ; Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учебное пособие. М. : Научно-издательский центр ИНФРА-М, 2017. С. 44.

[2] Решетников А. Ю. Квалификация неоконченных преступлений при наличии признаков совокупности преступлений // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2016. – № 4. – С. 85.

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

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

Состав по конструкции является материальным; преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. В отличие от ст. 274 УК РФ, характеризующейся двумя уровнями взаимосвязанных общественно опасных последствий, ч. 3 ст. 274.1 УК РФ не предполагает установления признака крупного ущерба.

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

Субъектом преступлений, предусмотренных чч. 1 и 2 ст. 274.1 УК РФ, является физическое вменяемое лицо, достигшее возраста 16 лет. Субъектом ч. 3 ст. 274.1 УК РФ может быть как общий – в части правил доступа к ресурсам, так и специальный – в части соблюдения правил эксплуатации соответствующих средств, систем и сетей.

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

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

Субъективная сторона преступления, предусмотренного ч. 3 ст. 274.1 УК РФ характеризуется двумя формами вины. Нарушение правил эксплуатации и доступа может совершаться как умышленно, так и по неосторожности. Следует поддержать точку зрения Н. Ш. Козаева, что неуказание на форму вины в составе нарушения правил эксплуатации средств хранения, обработки или передачи компьютерных данных (автор формулирует данный вывод применительно к ст. 274 УК РФ) является упущением законодателя, поскольку сама конструкция состава логически требует признания возможности совершения деяния по неосторожности, но ч. 2 ст. 24 УК РФ позволяет признавать преступление совершенным по неосторожности, только если это предусмотрено соответствующей статьей Особенной части УК РФ[1].

Квалифицированные виды неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, предусмотренные чч. 4 и 5 ст. 274.1 УК РФ, являются традиционными для преступлений в сфере компьютерной информа-

[1] Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства) : монография. М. : Юрлитинформ, 2015. С. 172.

ции и в целом хорошо освещены в современной литературе[1]. Дискуссионными, пожалуй, можно назвать два реализованных решения. Во-первых, законодатель проявил малопонятную последовательность в регламентации совершения преступления предварительно сговорившейся и организованной группами в рамках одной части. Очевидно, что уравнивание таких качественно разных по опасности форм соучастия вряд ли отвечает научно обоснованным критериям дифференциации ответственности. Во-вторых, все преступления в сфере компьютерной информации в качестве особо отягчающего обстоятельства называют наступление тяжких последствий или создание угрозы их наступления. Вместе с тем уголовно-правовая норма, предусмотренная ст. 274.1 УК РФ, такой оговорки не содержит, что, учитывая особую значимость объектов посягательства, представляется по меньшей мере ошибочным.

Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» предполагает категорирование всех объектов в зависимости от социальной, политической, экономической значимости, а также значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка. К сожалению, действующая редакция ст. 274.1 УК РФ не учитывает данное деление, что представляется существенным упущением не только с точки зрения игнорирования критериев дифференциации уголовной ответственности, но и что, пожалуй, более значимо, – анализируемая уголовно-правовая новелла не позволяет должным образом оценить различия в объеме и значимости социальных последствий криминальных посягательств на объекты критической инфраструктуры. Возможности учета опасности указанного деяния только лишь посредством дифференциации уголовного наказания, как представляется, явно недостаточны. Полагаем, что в этой части уголовно-правовая норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации требует корректировки.

§ 1.3. Особенности квалификации отдельных видов хищений, совершаемых с использованием информационно-коммуникационных технологий

Стремительная «цифровизация»[2] отечественной экономики помимо положительных аспектов с точки зрения повышения ее эффективности и конкурентоспособности, имеет, к сожалению, и свою негативную (криминогенную) сторону. Так преступники активно эксплуатируют незащищенность инновационных технологий, внедряемых в финансово-кредитную сферу, совершая посягательства на имущество граждан и ор-

[1] Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) // под ред. С. В. Дьякова, Н. Г. Кадникова. 5-е изд., перераб. и доп. М. : Юриспруденция, 2017. С. 822–834.

[2] Поветкина Н. А. Правовая форма интеграции информационных систем и информационных технологий в сферу публичных финансов // Журнал российского права. – 2018. – № 5. – С. 96–112 ; Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. – 2017. – № 10. – С. 5–18 ; Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. – 2018. – № 1. – С. 85–102.

ганизаций на принципиально новой (высокотехнологичной) основе. Так, по данным Национального агентства финансовых исследований (НАФИ) около половины российских компаний сталкивались с различными угрозами, а финансовые потери понесли 22 % из них, так средняя сумма убытков в одной компании составила 299 940 руб. В целом по стране потери от атак, совершаемых с использованием современных информационно-коммуникационных технологий, оцениваются в сумме свыше 116 млрд руб.[1]

Вместе с тем следует согласиться с утверждением А. Ю. Чупровой, что несмотря на наличие очевидных негативных аспектов, развитие электронной экономики невозможно затормозить[2]. В этом смысле она выступает как неизбежное будущее любого развитого государства.

Учитывая отрицательные последствия «цифровизации» деятельности хозяйствующих субъектов, российский законодатель принимает меры, направленные на формирование эффективного правового инструментария противодействия экономической киберпреступности. Так, с ноября 2012 г. отечественное уголовное законодательство пополнилось специальной нормой об ответственности за мошенничество в сфере компьютерной информации. С недавнего времени признаки компьютеризированного преступления приобрела кража. Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» ч. 3 ст. 158 УК РФ была дополнена новым особо квалифицирующим обстоятельством совершения кражи – с банковского счета, а равно в отношении электронных денежных средств. Аналогичный квалифицирующий признак был включен также в ч. 3 ст. 159.6 УК РФ. Кроме того, данным законом также были скорректированы название и диспозиция ст. 159.3 УК РФ путем указания на «электронные средства платежа». Отметим, что в целом указанная категория является более универсальной и охватывает не только платежные карты, но и иные современные средства безналичных расчетов с использованием информационно-коммуникационных технологий (Apple Pay, Samsung Pay и др.)[3].

Разработчики законопроекта указывали на то, что хищение денежных средств в электронной форме либо с банковского счета клиента, как правило, сопряжено с профессионализмом преступников, их оснащенностью и, как следствие, повышенной общественной опасностью[4]. В теории уголовного права было высказано соображение, что данное решение учитывает необходимость дополнительной защиты финансовых интересов граждан, кредитных организаций и государства в целом, а также предостав-

---

[1] Российские компании потеряли не менее 116 млрд руб. от кибератак в 2017 г. // URL: https://www.nafi.ru/analytics/rossiyskie-kompanii-poteryali-ne-menee-116-mlrd-rubley-ot-kiberatak-v-2017-godu/ (дата обращения: 30.01.2020).

[2] Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. … д-ра юрид. наук. М., 2015. С. 48.

[3] Легальное определение электронных средств платежа содержится в п. 19 ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», в соответствии с которым это средство и (или) способ, позволяют клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

[4] URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=159733&rnd=4C4C85B84AD6F5C60364116A6485AEF6#006814073483298333 (дата обращения: 05.01.2020).

ляет правоприменителям возможность задействовать весь спектр оперативно-разыскных мероприятий[1].

Опустив дискуссию о социально-правовой обусловленности внесенных в отечественный уголовный закон корректировок, необходимо обратить внимание, что реализация соответствующей законотворческой инициативы породила многочисленные вопросы в части отграничения кражи с банковского счета (п. «г» ч. 3 ст. 158 УК РФ) от общеуголовного мошенничества с использованием информационно-коммуникационных технологий и электронных средств платежа (ст. 159 УК РФ), мошенничества с использованием электронных средств платежа, в том числе банковских карт (ст. 159.3 УК РФ), а также мошенничества в сфере компьютерной информации, связанного с вмешательством в процессы нормального функционирования сервисов дистанционного банковского обслуживания (ст. 159.6 УК РФ).

В п. 1 постановления № 48 от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате» Пленум Верховного Суда Российской Федерации по-сути поставил точку в дискуссии относительно способа совершения преступления, предусмотренного ст. 159.6 УК РФ. Интерпретировав разъяснение высшей судебной инстанции, следует сделать вывод, что обман или злоупотребление доверием не являются способами мошенничества в сфере компьютерной информации.

Таким образом, получил поддержку подход, согласно которому преступление, предусмотренное ст. 159.6 УК РФ, характеризуется своим специфическим способом, не вписывающимся ни в одну из традиционно выделяемых форм хищения. Нельзя не отметить, что в первоначальной редакции п. 1 постановления Пленума состоял из двух абзацев и содержал специальное указание на то, что мошенничество в сфере компьютерной информации совершается не путем обмана или злоупотребления доверия, а иным способом – путем вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. Исключение данного разъяснения редакционной коллегией было мотивировано тем, что в теории уголовного права нет общепринятой позиции относительно того, является ли такое вмешательство разновидностью обмана или самостоятельным способом мошенничества[2]. Как представляется, проблема оценки манипуляций с компьютерной информацией как особого рода обмана имеет искусственный характер и обусловлена изначально неудачной редакций ст. 159.6 УК РФ. Название данной нормы, к сожалению, представляет собой не адаптированный к российской правовой системе, почти автоматизированный перевод ст. 8 «Компьютерное мошенничество» (Computer fraud) Конвенции «О преступности в сфере компьютерной информации» (Будапешт, 23 ноября 2001 г.)[3]. Учитывая многовековую отечественную традицию толкования природы мошенничества и обмана как способа его совершения, изначально правильнее было бы предусмотреть ответственность за «хищение в сфере компьютерной информации», как это реализовано, например,

---

[1] Иванов И. С., Рязанцева С. В. Современный подход к определению мер уголовной ответственности за хищение денежных средств, находящихся на банковском счете, и электронных денежных средств // Российский следователь. – 2018. – № 8. – С. 49.

[2] Заседание Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. // URL: http://www.vsrf.ru/press_center/news/26093/ (дата обращения: 06.12.2019).

[3] Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 г. // СПС «КонсультантПлюс». URL: https://www.consultant.ru.

в ст. 212 УК Республики Беларусь[1]. В сложившихся же условиях в ст. 159.6 УК РФ мы имеем новую форму хищения в сфере информационных технологий, которая мошенничеством не является, но называется таковым.

Пленум Верховного Суда Российской Федерации сделал обоснованный вывод, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа или создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст.ст. 272, 273, 274.1 УК РФ.

В соответствии с позицией Верховного Суда Российской Федерации, в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (например, злоумышленник тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», а затем авторизовался в системе интернет-платежей под известными ему данными другого лица), такие действия квалифицируются как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. Так, новые формы посягательства осуществляются преимущественно на электронные денежные средства граждан. Пленум предложил их квалифицировать как тайное хищение чужого имущества. Подобный подход вызывает ряд вопросов и требует некоторых замечаний. Прежде всего, объективно не всякое хищение, совершенное с использованием учетных данных, можно будет квалифицировать как кражу. Так, если соответствующая команда на списание денежных средств была отправлена открыто, в присутствии третьих лиц, не являющихся близкими виновному и осознававшими противоправный характер совершаемых действий, содеянное необходимо будет квалифицировать как грабеж.

Более того, если возможность воспользоваться телефоном потерпевшего возникла в результате нападения, сопряженного с применением насилия опасного для жизни или здоровья потерпевшего либо с угрозой его применения, и манипуляции с «мобильным банком» были осуществлены непосредственно в процессе нападения, содеянное будет охватываться составом разбоя. Полагаем, что как кражу можно будет квалифицировать действия лица, которое отправило команду на перевод денежных средств позднее, после нападения и завладения телефоном потерпевшего.

В некотором смысле анализируемое разъяснение Пленума нивелирует смысл и значение самостоятельного определения ст. 159.6 УК РФ. Оно распространяет действие ст. 158 УК РФ на такие часто встречающиеся в сети «Интернет» посягательства на электронные денежные средства граждан, совершенные в результате завладения учетными данными потерпевшего путем обмана («социальная инженерия»), создания сайтов-двойников («фишинг»), незаконного перевыпуска сим-карт и использования вредоносного программного обеспечения. С учетом последних разъяснений Пленума как мошенничество в сфере компьютерной информации следует оценивать хищения денежных средств граждан и организаций в результате использования вредоносных компьютерных программ.

---

[1] Уголовный кодекс Республики Беларусь (с изм. и доп. от 05.01.2015). Минск : Национальный центр правовой информации, 2015. С. 98.

Так, например, Бузин был осужден за совершение преступлений, предусмотренных ч. 2 ст. 273 УК РФ, ч. 2 ст. 272 УК РФ, ч. 2 ст. 159.6 УК РФ. В соответствии с приговором суда, Бузин, обладая достаточными познаниями в области компьютерной техники и навыками работы в сети «Интернет», приобрел путем копирования на накопитель своего персонального компьютера, программы, заведомо приводящие к несанкционированному доступу, уничтожению, блокированию, модификации, либо копированию информации. Функционально указанные программы были предназначены для управления удаленным компьютером по сети. После этого Бузин отправил на адрес электронной почты, используемого индивидуальным предпринимателем в своей финансовой деятельности, письмо свободного содержания, в которое под видом документа вложил указанные вредоносные программы. Продавец-консультант индивидуального предпринимателя, не подозревая о вредоносном содержании письма, используя служебный компьютер, открыл данное письмо, тем самым автоматически установив на компьютер вредоносную программу. Далее Бузин, незаконно используя вредоносные программы, без согласия и без ведома легального обладателя информации (индивидуального предпринимателя), из корыстной заинтересованности осуществил неправомерный доступ к компьютеру последнего, что вызвало блокирование компьютерной информации и сделало невозможным использование информации законным владельцем. После этого, продолжая свои преступные действия, направленные на мошенничество в сфере компьютерной информации, используя вредоносные свойства программ, посредством которых получил возможность ознакомиться с информацией о банковским счете и находящимися на нем денежными средствами, принадлежащими индивидуальному предпринимателю, Бузин осуществил перевод денежных средств потерпевшего на счет своего абонентского номера телефона, причинив значительный материальный ущерб[1].

Теоретически обоснованным и практически значимым следует признать разъяснение Пленума об оценке мошеннических действий в сети «Интернет» с использованием так называемой «социальной инженерии». В соответствии со вторым абзацем п. 21 постановления, если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет» (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159, а не ст. 159.6 УК РФ. Таким образом, принципиальным отличием общеуголовного мошенничества от компьютерного выступает наличие обмана или злоупотребления доверием потерпевшего, в результате чего он лично или через третьих лиц передает денежные средства или иное имущество злоумышленнику.

Следует отметить, что введение в заблуждение потерпевшего может быть следствием работы вредоносного программного обеспечения, что само по себе не исключает необходимость квалификации содеянного по ст. 159 УК РФ.

[1] Приговор Советского районного суда г. Улан-Удэ Республика Бурятия от 22 сентября 2015 г. по делу № 1-715/2015.

Так, спорным представляется решение суда по следующему делу. Братья Сдобновы были осуждены по ч. 2 ст. 159.6 УК РФ и ч. 2 ст. 273 УК РФ. Согласно материалам дела, виновные создали в сети «Интернет» сайты, в стартовый файл которых были заранее интегрированы вредоносные программы, заведомо предназначенные для блокирования функций операционной системы персональных компьютеров. Одновременно с блокированием пользователям приходили сообщения якобы от правоохранительных органов (МВД России, Управления «К» МВД России и др.), содержащие сведения о необходимости перечисления денежных средств по соответствующим реквизитам в качестве оплаты наложенного на пользователя сети «Интернет» административного штрафа за просмотр и копирование материалов порнографического содержания. Полученные от потерпевших денежные средства Сдобновы в дальнейшем тратили на собственные нужды[1].

Учитывая, что денежные средства списывались вредоносной программой не автоматически, а перечислялись потерпевшими самостоятельно в качестве оплаты несуществующих административных штрафов за просмотр порнографических материалов, содеянное, на наш взгляд, подпадает под действие общей нормы о мошенничестве (ст. 159 УК РФ).

Как известно, Пленум скорректировал традиционный подход к определению момента окончания хищения, если его предметом выступали безналичные денежные средства, в том числе электронные денежные средства. Согласно новой позиции такое хищение следует считать оконченным не с момента зачисления денежных средств на счет виновного или третьих лиц, а с момента их изъятия у владельца (п. 5). Данное решение Пленума было продиктовано двумя обстоятельствами:

– редакционная коллегия отметила, что высокий уровень развития товарно-денежных отношений, информационных технологий и банковских услуг позволяет за считанные минуты осуществлять перевод и зачисление денежных средств, оплату товаров и др. В связи с этим с момента списания денежных средств со счета потерпевшего у виновного появляется реальная возможность по их беспрепятственному распоряжению;

– в отдельных случаях у правоохранительных органов не всегда имеется возможность достоверно установить, куда были перечислены похищенные денежные средства потерпевшего, что само по себе не должно влиять на квалификацию мошенничества как оконченного преступления[2].

Указанное разъяснение высшей судебной инстанции в целом следует оценить положительно. Как известно, случаи неверного толкования момента окончания компьютерного мошенничества на практике встречались. Например, как покушение на компьютерное мошенничество были квалифицированы действия лиц, которые были задержаны в отделении банка уже при попытке получения похищенных денежных средств с расчетного счета фирмы-однодневки, куда были перечислены похищенные денежные средства юридического лица в результате заражения вредоносным программным обеспечением служебного компьютера организации с установленной си-

[1] Приговор Первомайского районного суда Оренбургской области от 8 июля 2016 г. по делу № 1-58/2016.

[2] Заседание Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. // URL: http://www.vsrf.ru/press_center/news/26093/ (дата обращения: 06.12.2019).

стемой «Банк-Клиент»[1]. Вместе с тем ошибочно полагать, что данное разъяснение не может иметь исключений. На наш взгляд, несмотря на положения пункта 5 нового постановления Пленума, как покушение на мошенничество в сфере компьютерной информации следует оценивать ситуации, когда в рамках оперативно-разыскных мероприятий по запросу правоохранительных органов финансовая организация заранее приостановила любые расходные операции по счету, на который впоследствии были зачислены похищенные злоумышленниками денежные средства.

Принятие Федерального закона от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» некоторым образом нивелировало значимость официальных рекомендаций Пленума Верховного Суда Российской Федерации о квалификации специальных видов мошенничества, содержащихся в Постановлении № 48 от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате», в которых, по справедливому мнению А. Г. Кибальника, заключалась его главная правоприменительная ценность[2]. После апрельских изменений отечественного уголовного закона правоприменитель опять оказался в ситуации частичной неопределенности и прежде всего в вопросе разделения посягательств на электронные денежные средства граждан и денежные средства, хранимые на банковских счетах.

Полагаем, что для решения вопроса об отграничении «электронной кражи» от вышеуказанных составов преступлений следует исходить из того, какую роль играл тот или иной способ в механизме совершения посягательства.

Следует согласиться с А. А. Лебедевой, что в случаях, когда лицо похитило денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного следует квалифицировать как кража[3].

Анализ судебной практики показывает, что по п. «г» ч. 3 ст. 158 УК РФ оцениваются действия лица, которое завладело платежной картой потерпевшего и осуществило изъятие денежных средств в наличной форме через устройство самообслуживания клиентов.

Так, М. был осужден по п. «г» ч. 3 ст. 158 УК РФ. В соответствии с приговором суда М., используя предварительно изъятую у потерпевшей банковскую карту, а также информацию о пин-коде, которую потерпевшая сообщила М. ранее, через банкомат осуществил четыре операции по обналичиванию денежных средств с банковского счета в размере 33 864 руб., чем причинил потерпевшей значительный материальный ущерб[4].

---

[1] Приговор Пресненского районного суда г. Москвы от 23 января 2014 г. по делу № 1-43/2014.

[2] Кибальник А. Г. Квалификация мошенничества в новом постановлении Пленума Верховного Суда Российской Федерации // Уголовное право. – 2018. – № 1. – С. 61.

[3] Лебедева А. А. Актуальные вопросы квалификации мошенничества в сфере компьютерной информации // Безопасность бизнеса. – 2018. – № 5. – С. 47.

[4] Приговор Ленинского районного суда г. Смоленска от 20 сентября 2018 г. по делу № 1-275/2018.

Компьютеризация состава кражи заставляет несколько переосмыслить обоснованный в теории уголовного права подход, согласно которому «ст. 159 УК РФ должна применяться в случаях, когда использование способов: ввода, удаления, блокирования компьютерной информации и т. д. – приводит к переводу денежных средств с одного счета на другой, контролируемый виновным счет»[1]. В современной редакции ст. 158 УК РФ такое толкование является обоснованным только в том случае, если манипуляции с компьютерной информацией (ввод, модификация и т. д.) привели не просто к перемещению денежных средств, но и повлекли нарушение нормальной работы объектов информационно-коммуникационной инфраструктуры (например, блокировке личного кабинета потерпевшего в системе дистанционного банковского обслуживания). При отсутствии таких последствий, содеянное необходимо квалифицировать по п. «г» ч. 3 ст. 158 УК РФ. Подобный подход находит свое отражение и в правоприменительной практике.

Так, в решении суда по уголовному делу в отношении Д., квалифицировавшем содеянное по п. «г» ч. 3 ст. 158 УК РФ, виновный, получив во временное пользование телефон потерпевшего, в котором было установлено приложение дистанционного банковского обслуживания и убедившись, что потерпевший отвлечен и за его преступными действиями не наблюдает, осуществил перевод денежных средств в сумме 17 000 руб., принадлежащих потерпевшему[2].

Изучение имеющейся судебно-следственной практики показывает, что действия, связанные с оплатой товаров и услуг, довольно часто квалифицируются как кража с банковского счета.

Так, по п. «г» ч. 3 ст. 158 УК РФ были квалифицированы действия лица, которое, воспользовавшись отсутствием потерпевшего, изъяло принадлежащую ему банковскую карту. После чего в продолжение своего преступного умысла, находясь в магазине, трижды осуществило оплату приобретенного товара банковской картой на суммы: 591 руб. 06 коп., 354 руб., 970 руб. 82 коп. Примерно в это же время, находясь уже в другом магазине, дважды осуществило оплату приобретенного товара банковской картой потерпевшего на суммы: 151 руб. 80 коп., 105 руб.[3]

Изменив диспозицию ст. 159.3 УК РФ, законодатель по каким-то причинам исключил оговорку о том, что соответствующие действия должны быть сопряжены с обманом уполномоченного работника кредитной или иной организации. Если согласиться с тем, что такой способ уже не является обязательным, то данный состав преступления станет абсолютно неотличимым от кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ). В связи с этим полагаем, что толкование данного преступления по-прежнему должно основываться на

---

[1] Тюнин В. Мошенничество в сфере компьютерной информации: сложности квалификации // Уголовное право. – 2017. – № 5. – С. 95.

[2] Приговор Центрального районного суда г. Воронежа от 25 октября 2018 г. по делу № 1-312/2018.

[3] Приговор Домодедовского городского суда Московской области от 6 ноября 2018 г. по делу № 1-399/2018.

разъяснениях, сформулированных в п. 17 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которым признаки ст. 159.3 УК РФ имеют место только в случаях, когда хищение имущества осуществлялось путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности лицу карты (с учетом изменений – электронного средства платежа) на законных основаниях либо путем умолчания о незаконном владении им такой картой (с учетом изменений – электронным средством платежа).

Так, осуществляя переквалификацию с п. «г» ч. 3 ст. 158 УК РФ на ст. 159.3 УК РФ, суд, ссылаясь на указанное выше разъяснение Пленума, обосновывает вывод, что поскольку А., реализуя свой преступный умысел, совершил хищение денежных средств потерпевшего путем умолчания перед продавцом о незаконном владении им платежной картой, оплатив ряд покупок безналичным путем, используя систему «ПайПасс», содеянное является мошенничеством с использованием электронных средств платежа, а не кражей с банковского счета[1].

По другому делу суд согласился с позицией обвинения о наличии в действиях виновного совокупности преступлений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ и ч. 2 ст. 159.3 УК РФ, ссылаясь на то, что лицо совершило как изъятие денежных средств потерпевшего посредством банкомата, так и, «выдавая себя за собственника банковской карты, обманывая работника торговой организации» произвело оплату купленных товаров[2].

По мнению З. И. Хисамовой, имеющаяся в законе оговорка «при отсутствии признаков преступления, предусмотренного ст. 159.3» выражается в том, что неправомерный доступ к счету или электронному кошельку был получен и осуществлен без применения специальных информационно-телекоммуникационных технологий (скиммеров, банковских троянов и др.)[3]. При этом в обоснование собственного подхода автор отдельно оговаривает, что основное отличие кражи от мошенничества с использованием электронных средств платежа заключается именно в способе хищения. Для квалификации деяния как мошенничества с использованием электронного средства платежа необходимо целенаправленное воздействие на программное обеспечение, приложение, устройство, позволяющее получить неправомерный доступ к счету владельца[4].

Как представляется, данная точка зрения является дискуссионной. Подобное видение объективной стороны мошенничества с использованием электронных средств пла-

---

[1] Приговор Ново-Савинского районного суда г. Казани от 16 ноября 2018 г. по делу № 1-525/2018.

[2] Приговор Муромского городского суда Владимирской области от 30 ноября 2018 г. по делу № 1-297/2018.

[3] Хисамова З. И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики // Российский следователь. – 2018. – № 9. – С. 46.

[4] Там же.

тежа делает его неотличимым от мошенничества в сфере компьютерной информации. Как уже отмечалось ранее, в отличие от кражи с банковского счета и мошенничества с использованием электронных средств платежа компьютерное мошенничество, предусмотренное ст. 159.6 УК РФ, предполагает неправомерное вмешательство в процесс нормального функционирования объектов информационно-коммуникационной инфраструктуры (п. 20 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

Типичным примером мошенничества в сфере компьютерной информации может выступать следующее решение суда по уголовному делу.

Так, Ж., выполняя свою роль в преступной группе, установил на терминал по приему платежей от населения программу удаленного администрирования, а также вредоносную компьютерную программу. После чего Ж., убедившись в том, что при помощи установленной им программы можно осуществить удаленный доступ к терминалу, покинул торговое помещение. В этот же день, находясь по месту своего проживания, Ж. в сервисе мгновенного обмена сообщениями отправил неустановленный идентификационный номер А., который, выполняя свою роль в преступной группе, произвел подключение к программе удаленного администрирования, установил в память терминала: программное обеспечение, позволяющее подтвердить принятие денежной купюры в устройстве, предназначенном для проверки купюр (валидаторе), при ее действительном отсутствии, а также другие программы, обеспечивающие настройку и корректную работу программного обеспечения, позволяющего подтвердить принятие денежной купюры в устройстве, предназначенном для проверки купюр (валидаторе), при ее действительном отсутствии, то есть осуществил модификацию компьютерной информации. После чего А., имея возможность удаленно управлять программными продуктами, установленными им в терминал по приему платежей от населения, незаконно, путем ввода и модификации компьютерной информации, осуществил 8 переводов денежных средств на общую сумму 35 300 руб. со специального счета терминала по приему платежей от населения на счет в одной из электронных платежных систем[1].

Как мошенничество в сфере компьютерной информации, на наш взгляд, также следует оценивать действия злоумышленника, который изымает в наличной форме денежные средства из устройства самообслуживания клиентов банка (банкомата, терминала оплаты и др.) посредством неправомерного вмешательства в его функционирование с использованием вредоносных компьютерных программ (так называемые атаки типа «black box», при которых лицо просверливает отверстие в банкомате, подключается через USB-порт и использует вредоносное программное обеспечение, чтобы дать команду на выдачу денежных средств). В данном случае изъятие денежных средств имеет не примитивно-бытовой характер, а реализуется способом, который напрямую описан в диспозиции ст. 159.6 УК РФ – путем ввода и модификации компьютерной информации в программном обеспечении банкомата. При этом следует, конечно же, оговориться, что

[1] Приговор Советского районного суда г. Орска Оренбургской области от 17 августа 2018 г. по делу № 1-240/2018.

простое изъятие купюроприемника с сейфом в результате повреждения банкомата должно оцениваться как кража (однако без применения п. «г» ч. 3), либо в зависимости от обстоятельств содеянного – как грабеж либо разбой.

Сложности в оценке деяний имеют место в случаях отграничения кражи с банковского счета от общеуголовного мошенничества, в результате которого потерпевший самостоятельно перечисляет денежные средства, используя сервисы дистанционного банковского обслуживания.

Так, Н. была осуждена по ч. 2 ст. 159 УК РФ. В соответствии с приговором суда, Н., имея умысел на хищение чужого имущества, принадлежащего Ш., под надуманным предлогом продажи товара, заведомо осознавая, что товар Ш. не предоставит, а полученные в качестве оплаты денежные средства обратит в свою пользу, путем обмана получила со счета зарегистрированной на Ш. банковской карты принадлежащие Ш. и предназначавшиеся в качестве оплаты за товар денежные средства в размере 15 500 руб., после чего распорядилась ее деньгами по своему усмотрению, причинив Ш. значительный материальный ущерб на общую сумму 15 500 руб.[1].

Принципиальным отличием общеуголовного мошенничества с использованием методов так называемой «социальной инженерии» от кражи с банковского счета потерпевшего выступает наличие обмана или злоупотребления доверием потерпевшего, в результате чего он лично или через третьих лиц передает денежные средства или иное имущество злоумышленнику. Следовательно, в распространенных случаях введения клиентов банков в заблуждение по телефону, когда виновный представляется работником службы безопасности финансовой организации либо социальным работником, необходимо установить в результате каких действий денежные средства были списаны со счета. Если виновный стремился к тому, чтобы клиент совершил соответствующие манипуляции с платежной картой и тем самым самостоятельно перевел денежные средства на счет злоумышленника, содеянное образует признаки общеуголовного мошенничества. В тех же случаях, когда лицо обманным путем лишь получает сведения о платежной карте либо другую критически значимую информацию, касающуюся работы сервисов дистанционного банковского обслуживания (например, одноразовый код-пароль для входа в систему), и, как это бывает на практике, не прерывая разговора с потерпевшим, параллельно совершает операции по изъятию денежных средств с банковского счета, содеянное необходимо квалифицировать по п. «г» ч. 3 ст. 158 УК РФ.

Дискуссионным является вопрос об отграничении мошенничества в сфере компьютерной информации от присвоения и растраты с использованием сервисов дистанционного банковского обслуживания (например, когда бухгалтер совершает хищение денежных средств путем отправки подложного платежного поручения в электронной форме). В теории уголовного права отмечается, что независимо от того, являлся ли преступник материально ответственным лицом, а похищаемое имущество было вверенным ему, такие действия все равно следует квалифицировать по ст. 159.6 УК РФ, если имело место использование компьютерной информации или информационно-

[1] Приговор Солнцевского районного суда г. Москвы от 6 ноября 2018 г. по делу № 1-318/18.

коммуникационных сетей[1]. Примеры из судебно-следственной практики[2] также демонстрируют тенденцию оценки таких действий по ст. 159.6 УК РФ. На наш взгляд, с учетом разъяснений постановления Пленума содеянное необходимо квалифицировать по ст. 160 УК РФ по причине специфического содержания предмета хищения – на момент изъятия имущество является вверенным виновному.

До конца нерешенным является вопрос относительно квалификации действий виновного, который совершил хищение денежных средств банка при автоматизированном процессе получения кредита, то есть без непосредственного контакта с менеджером, когда платежеспособность клиента проверяет компьютер в автоматическом режиме (с помощью терминала экспресс-кредитования). Принимая во внимание, что предметом хищения в таком случае выступает денежные средства, предоставляемые в рамках кредитного договора, совершенные лицом действия справедливо могут рассматриваться как мошенничество в сфере кредитования (ст. 159.1 УК РФ). С другой стороны, учитывая, что способ совершения преступления был связан с вводом компьютерной информации, есть убедительные основания, чтобы квалифицировать содеянное как компьютерное мошенничество по ст. 159.6 УК РФ.

Проблема с конкуренцией компьютерного мошенничества возникает и в случаях, когда заведомо ложное заявление о наступлении страхового случая, а равно иные документы предоставляются страховщику в электронной форме посредством использования сети «Интернет». С одной стороны, независимо от способа коммуникации с работниками страховой компании содеянное образует мошенничество в сфере страхования (ст. 159.5 УК РФ). Вместе с тем, если принятие решения о выплате страхового возмещения будет осуществляться автоматически компьютерной программой, то содеянное уже в большей мере будет соответствовать признакам мошенничества в сфере компьютерной информации.

---

[1] Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике / С. Н. Потапкин [и др.]. – URL : https://base.garant.ru/57488207.

[2] Приговор Хамовнического районного суда г. Москвы от 15 мая 2014 г. по делу № 1-49/2014 ; Приговор Салаватского городского суда Республики Башкортостан от 21 мая 2015 г. по делу № 1-113/2015.

ГЛАВА II. ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ

§ 2.1. Использование систем дистанционного обслуживания

Высокая конкуренция в кредитно-финансовой сфере заставляет кредитные организации использовать инновационные финансовые технологии для создания конкурентных преимуществ и повышения эффективности своей деятельности. Активное внедрение и использование кредитными организациями инновационных финансовых технологий является на сегодняшний день одним из важнейших фактором обеспечения стабильности функционирования кредитной организации в условиях конкурентной среды.

Одним из приоритетных направлений обеспечения конкурентных преимуществ и повышения эффективности деятельности на долгосрочный период является активное внедрение и использование дистанционный технологий обслуживания клиентов.

Дистанционное обслуживание кредитными организациями своих клиентов представляет собой способ предоставления клиентам кредитной организации, физическим и юридически лицам, банковских услуг без непосредственного посещения отделения кредитной организации, а с использованием различных каналов связи.

Использование кредитной организацией различных каналов взаимодействия со своими клиентами при дистанционном обслуживании позволяет получать клиентам не только весь спектр традиционных банковских услуг, доступных в отделениях кредитной организации, но и предоставляет возможность на ином качественном уровне удовлетворять потребности своих клиентов.

К наиболее распространенным на сегодняшний день каналам связи между кредитной организацией и ее клиентами относится телефонная и мобильная связь, связь посредством локальных сетей или сети «Интернет», а также банковские устройства самообслуживания: банкоматы и терминалы.

За последние несколько лет существенно увеличилось количество клиентов кредитных организаций, которые активно пользуются технологиями дистанционного обслуживания при получении банковских услуг. При этом некоторые физические и юридические лица могут являться клиентами сразу нескольких кредитных организаций. Процесс активного использования клиентами кредитных организаций технологий дистанционного обслуживания обусловлен теми преимущества, которые они получают. При этом необходимо отметить, что дистанционное обслуживание является выгодной и эффективной формой взаимодействия как для кредитной организации, так и для ее клиентов.

Рассмотрим преимущества и недостатки использования дистанционного обслуживания для кредитных организаций и их клиентов.

К основным преимуществам использования технологий дистанционного обслуживания для кредитных организаций можно отнести:

– финансовые преимущества, которые связаны с сокращением затрат на обслуживание клиентов с использованием технологий дистанционного обслуживания по сравнению с обслуживанием в отделениях кредитной организации, за счет сокращения затрат на содержание отделения кредитной организации, оплату труда персонала и т. п.;

расширением клиентской базы кредитной организации вне зависимости от географического местоположения новых клиентов;

– конкурентные преимущества, которые возникают за счет повышения удовлетворенности клиентов качеством своего банковского обслуживания, в том числе проявляющееся в возможности оперативного доступа клиента к информации, касающейся осуществляемых операций, информации по счетам и т. п.; снижения риска ошибок при проведении банковских операций клиентами самостоятельно, в связи с использованием унифицированных шаблонов для проведения банковских операций и т. д.

К основным преимуществам использования технологий дистанционного обслуживания для клиентов кредитных организаций можно отнести:

– удобство использования, проявляющееся в экономии клиентом своего личного времени в связи с отсутствием необходимости посещать отделение кредитной организации, тратить время на нахождение в очереди и т. д.; возможность совершать банковские операции и пользоваться банковскими услугами в любое время и находясь в любом месте;

– выгода использования, проявляющаяся в дифференциации тарифов на проведение банковских операций в отделениях кредитной организации и в системе дистанционного обслуживания, как правило, тарифы при дистанционном обслуживании ниже тарифов при непосредственном обслуживании в отделении кредитной организации; операции, совершаемые с использованием технологий дистанционного обслуживания, как правило, осуществляются в очень короткие промежутки времени, а иногда и вовсе моментально.

Таким образом, внедрение и использование кредитными организациями технологий дистанционного обслуживания своих клиентов предоставляет возможность на качественно ином уровне удовлетворять потребности клиентов в банковских услугах. Для клиентов появляется возможность проводить банковские операции и пользоваться банковскими услугами в режиме реального времени, что существенно позволяет экономить личное время. Для банков появляется возможность оптимизировать свои издержки и сформировать дополнительные конкурентные преимущества.

Однако, необходимо указать, что наряду с перечисленными преимуществами использование дистанционного обслуживания не лишено и недостатков. К основным недостаткам можно отнести:

Большие первоначальные затраты на создание и внедрение системы дистанционного обслуживания клиентов, а также на ее обслуживание. С одной стороны, окупаемость затрат на разработку и внедрение системы дистанционного обслуживания обеспечивается при увеличении количества клиентов, пользующихся дистанционным обслуживанием. С другой стороны – при наличии ошибок в планировании затрат на разработку, внедрение и обслуживание системы дистанционного обслуживания, связанном с количеством клиентов, пользующихся дистанционным обслуживанием, кредитной организации не удастся возместить понесенные затраты. Поэтому внедрять системы дистанционного обслуживания клиентов экономически целесообразно только при возможности привлечения кредитной организацией достаточного количества клиентов, которые будут пользоваться дистанционным обслуживанием.

Высокие риски мошеннических действий и кибератак на системы дистанционного обслуживания клиентов. Высокая доходность и относительно низкий риск разоблачения способствуют активному увеличению количества киберпреступлений, совершаемых в кредитно-финансовой сфере. Как правило, кибератаки совершаются на системы межбанковских переводов, карточный процессинг, управление банкоматами, интернет-банкинг, платежные шлюзы. В добавок, на сегодняшний день, уже функционирует сложившийся рынок криминальных киберуслуг. На специализированных форумах в DarkNet практически любой желающий может беспрепятственно приобрести вредоносное программное обеспечение с подробными инструкциями по его использованию для совершения кибератаки на кредитные организации.

На сегодняшний день основными видами систем дистанционного обслуживания клиентов, используемых кредитными организациями, являются: система «Банк-клиент», интернет-банкинг, мобильный банкинг и внешние сервисы.

Систем «Банк-клиент» представляет собой банковскую программу, которая устанавливается на компьютер клиента и предназначена для удаленного осуществления платежей и других банковских операций, а также контроля расчетного счета в режиме реального времени посредством обмена информацией с банковским сервером через интернет.

Основные возможности системы «Банк-клиент», предоставляемые в настоящее время:

– осуществлять переводы;

– получать детальную информацию о движении денежных средств и остатках на расчетном счете;

– просматривать статус отправленных платежей;

– импортировать и экспортировать платежные документы из бухгалтерских систем;

– покупать и продавать иностранную валюту;

– отправлять в банк любые документы в электронном виде;

– использовать экспресс-сервис проверки контрагентов;

– получать документы, подтверждающие проведение операций по расчетному счету.

Необходимо отметить, что на сегодняшний день большинство систем «Банк-клиент» позволяют осуществлять обмен электронными документами между учетной системой клиента и банка с использованием соответствующего интеграционного модуля, что позволяет формировать и отправлять в банк электронных документов в привычном интерфейсе учетной системы клиента.

Интернет-банкинг представляет собой вид дистанционного обслуживания как частных, так и корпоративных клиентов с предоставлением им доступа к собственным счетам и услугам банка посредством сети «Интернет».

Интернет-банкинг предоставляет широкие возможности, среди которых:

– осуществление переводов;

– осуществление платежей различного рода;

– просмотр истории операций, поступлений и списаний с детализацией за выбранный период.

Мобильный банкинг представляет собой вид дистанционного обслуживания, предоставляющий возможность получения информации и управления средствами на банковском счете с помощью мобильного телефона.

Внешние сервисы – это вид дистанционного обслуживания с использованием устройств банковского самообслуживания (банкоматов и платежных терминалов).

Банкомат представляет собой автоматизированный аппарат с программным обеспечением, предназначенный для выполнения наличных операций (прием/выдача) и некоторых других функций. Кроме того, в такую машину обязательно встроены принтер, компьютер, модемы, картридер, клавиатура, сейф и монитор. Имеется постоянная связь с процессингом обслуживающего банка – осуществляется через сеть интернет.

Терминал представляет собой аппарат с программным обеспечением, предназначенный для проведения операций в режиме самообслуживания. Помимо разного внешнего вида еще одним существенным отличием является работа с наличностью: терминал не выдает деньги, а только принимает их.

Существуют два вида терминалов:

– информационно-платежные – ориентированы, помимо платежей, на ряд других функций, к примеру: подключение к СМС-информированию, распечатка мини-выписок и т. д.;

– платежные – ориентированы исключительно на осуществление платежей.

§ 2.2. Основные риски и киберугрозы кредитных организаций, связанные с использованием систем дистанционного обслуживания

Кредитные организации стремятся использовать передовые финансовые технологии, с целью предоставления своим клиентам возможности удаленно получать банковские услуги. В настоящее время для получения большинства банковских услуг достаточно оформить банковскую карту и заключить договор о дистанционном банковском обслуживании. Появляются даже кредитные организации, которые отказались от предоставления своим клиентам обслуживания в своих территориальных отделениях, но при этом оказывают полный спектр банковских услуг дистанционно. Данный подход предоставляет множество преимуществ как кредитным организациям, так и их клиентам: для клиентов – это прежде всего удобство и скорость получения соответствующих банковских услуг; для кредитной организации – сокращение практически всех видов затрат, связанных с содержанием территориальных отделений.

Однако есть у данного процесса и обратная сторона – необходимость обеспечивать безопасность и минимизировать риски, связанные с использованием систем дистанционного обслуживания.

На сегодняшний день кредитно-финансовая сфера является одной из самых привлекательных для киберпреступников. Активное внедрение в последние несколько лет в практику работы кредитных организаций систем дистанционного обслуживания своих клиентов и постоянное расширение услуг, предоставляемых с помощью дистанционного обслуживания привело к тому, что к настоящему времени киберриски стали для кредитных организаций одними из самых значимых, которые могут представлять серьезную угрозу их финансовой стабильности.

ФинЦЕРТ[1] Банка России указывает, что на сегодняшний день отдельные киберриски кредитных организаций порождают риски в кредитно-финансовой сфере в целом в связи с тем, что:

– финансовые потери клиентов (потребителей финансовых услуг), подрывают доверие к современным финансовым технологиям;

– финансовые потери отдельных финансовых организаций, способны оказать существенное негативное (критическое) воздействие на их финансовое положение;

– нарушение операционной надежности и непрерывности предоставления финансовых услуг, приводит к репутационному ущербу и нарастанию социальной напряженности в обществе;

– возможно развитие системного кризиса в случае возникновения инцидентов информационной безопасности вследствие кибератак в значимых для финансового рынка организациях.

Одним из главных мотивов киберпреступников является получение финансовой выгоды от организации и проведения кибератаки на кредитные организации. При этом начиная с 2018 г. отмечается рост доли инцидентов, которые нацелены на получение информации о платежных картах, персональных данных клиентов, учетных данных пользователей систем дистанционного обслуживания для доступа к личным кабинетам, которые в дальнейшем так же позволяют извлекать финансовую выгоду за счет последующей кражи денежных средств со счетов клиентов финансово-кредитных организаций или же продажи этих конфиденциальных данных на специализированных сервисах в DarkNet.

К основным объектам для кибератак на организации кредитно-финансовой сферы можно отнести системы межбанковских переводов, процессинговые системы, платежные шлюзы, дистанционный банкинг и инфраструктуру управления банкоматами.

Любая киберпреступная группировка использует множество различных способов для организации и проведения кибератаки, но, как правило, все они включают в себя следующие этапы:

– сбор информации о кредитной организации, в отношении которой планируется проведение кибератаки;

– проникновение во внутреннюю сеть этой организации;

– закрепление во внутренней сети этой организации;

– получение доступа к управлению финансовыми системами и хищение денежных средств со счетов;

– сокрытие следов хищения.

По данным исследования компании Positive Technologies в 2018–2019 гг., основными методами кибератак на кредитные организации являлись:

– использование вредоносного программного обеспечения;

– использование методов социальной инженерии;

– хакинг;

---

[1] ФинЦЕРТ – центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере – структурное подразделение Департамента информационной безопасности. По данным на 2018 г. в рамках ФинЦЕРТ взаимодействуют более 600 банков.

– подбор учетных данных пользователей;
– эксплуатация веб-уязвимостей.

При этом киберпреступники нередко комбинируют эти методы в ходе кибератаки на кредитные организации.

Специалисты по кибербезопасности отмечают, что сегодня наличие вредоносного программного обеспечения стало обязательным элементом, без которого практически невозможна ни одна кибератака, поскольку оно позволяет решать задачи, связанные эффективностью проведения кибератаки.

В зависимости от назначения вредоносное программное обеспечение подразделяется на несколько типов:

– криптомайнеры (cryptojacking);
– трояны для кражи данных (stealer);
– хакерские инструменты;
– вредоносное программное обеспечение для DDoS;
– трояны-вымогатели (ransomware);
– трояны удаленного доступа (RAT);
– трояны-загрузчики (loader, dropper);
– вредоносное программное обеспечение для создания ботнета;
– вредоносное программное обеспечение для банкоматов.

В крупных кредитных организациях, как правило, система обеспечения кибербезопасности хорошо организована. Поэтому киберпреступниками для проникновения в финансовую инфраструктуру используются методы социальной инженерии. Одним из эффективных способов доставки вредоносного программного обеспечения на этапе проникновения в организацию является фишинг. При этом нефинансовые компании и кредитные организации, где система обеспечения кибербезопасности не достаточно эффективна, могут использоваться киберпреступниками как промежуточные звенья кибератаки для рассылки с зараженных компьютеров этих организаций фишинговых писем в адрес крупных кредитных организаций.

Необходимо отметить, что активно развивается и криминальный рынок киберуслуг, который позволяет киберпреступникам не разрабатывать свое собственное вредоносное программное обеспечение, а покупать уже готовые решения для организации кибератак на кредитные организации. При этом возможность приобретения киберпреступными группировками готового вредоносного программного обеспечения для кибератак на кредитные организации позволяет утверждать, что вредоносное программное обеспечение будет и дальше широко использоваться киберпреступниками в атаках на кредитные организации.

Социальная инженерия представляет собой преднамеренное введение в заблуждение путем обмана или злоупотребления доверием, как правило, для получения конфиденциальных данных или доступа к ним с целью последующего хищения денежных средств со счета клиента. Киберпреступники легко модифицируют используемые методы социальной инженерии в процессе ее при для достижения своих целей.

ФинЦЕРТ Банка России в результате анализа средств и методов социальной инженерии сделал вывод о том, что основным объективным факторам, который способствует распространению социальной инженерии, является неправомерный доступ и

обработка персональных данных клиентов кредитных организаций. Так, для хищения денежных средств методом социальной инженерии мошенникам достаточно владеть информацией о фамилии, имени и отчестве, а также о номере телефона клиента кредитной организации. При этом данные, относящиеся к банковской тайне, необязательны для совершения противоправных действий. Мошенники лишь уточняют и дополняют необходимую информацию, которая в дальнейшем позволяет им похитить денежные средства со счета клиента.

Данным обстоятельством как раз может объясняться тенденция, связанная с ростом доли инцидентов, которые нацелены на получение информации о платежных картах, персональных данных клиентов, учетных данных пользователей систем дистанционного обслуживания для доступа к личным кабинетам и т. д.

Хакинг представляет собой преднамеренное внесение изменений в программное обеспечение для достижения определенных целей, которые отличаются от целей разработчиков и пользователей данного программного обеспечения.

Хакинг предполагает эксплуатацию киберпреступникам как известных уязвимостей, так и уязвимостей нулевого дня в программном обеспечении, которое используют кредитные организации и их клиенты, в целях хищения денежных средств. Одним из способов противодействия хакингу является своевременное обновление используемого программного обеспечения. Однако довольно большое количество организаций и физических лиц своевременно не устанавливают обновления и в первую очередь становятся жертвами соответствующих кибератак.

Подбор учетных данных пользователей представляет собой различные алгоритмы подбора пароля пользователя.

Эксплуатация веб-уязвимостей предполагает использование уязвимостей веб-страниц и веб-приложений, чаще всего с помощью вредоносного скрипта или программы (эксплойта).

§ 2.3. Поиск цифровых следов в системах дистанционного банковского обслуживания

В последнее время участились случаи хищения денежных средств из банковских устройств самообслуживания и систем дистанционного банковского обслуживания. Преступники, совершенствуя свои технические знания, перешли от классических способов хищения (путем взрыва, взлома, распила банкомата) к более технологическим способам (например, заражение технических устройств вредоносными программами). Таким образом при выявлении, раскрытии и расследовании данных преступлений важным представляется обнаружение и фиксация цифровых следов.

Вход в интернет-банкинг

Для входа в Internet-Банкинг выполните:

Подключитесь к Интернету, запустите Web-браузер и перейдите на страницу входа корпоративных клиентов системы «iBank 2» вашего банка, рис. 2.3.1 – URL: https://ibank.sit.local.

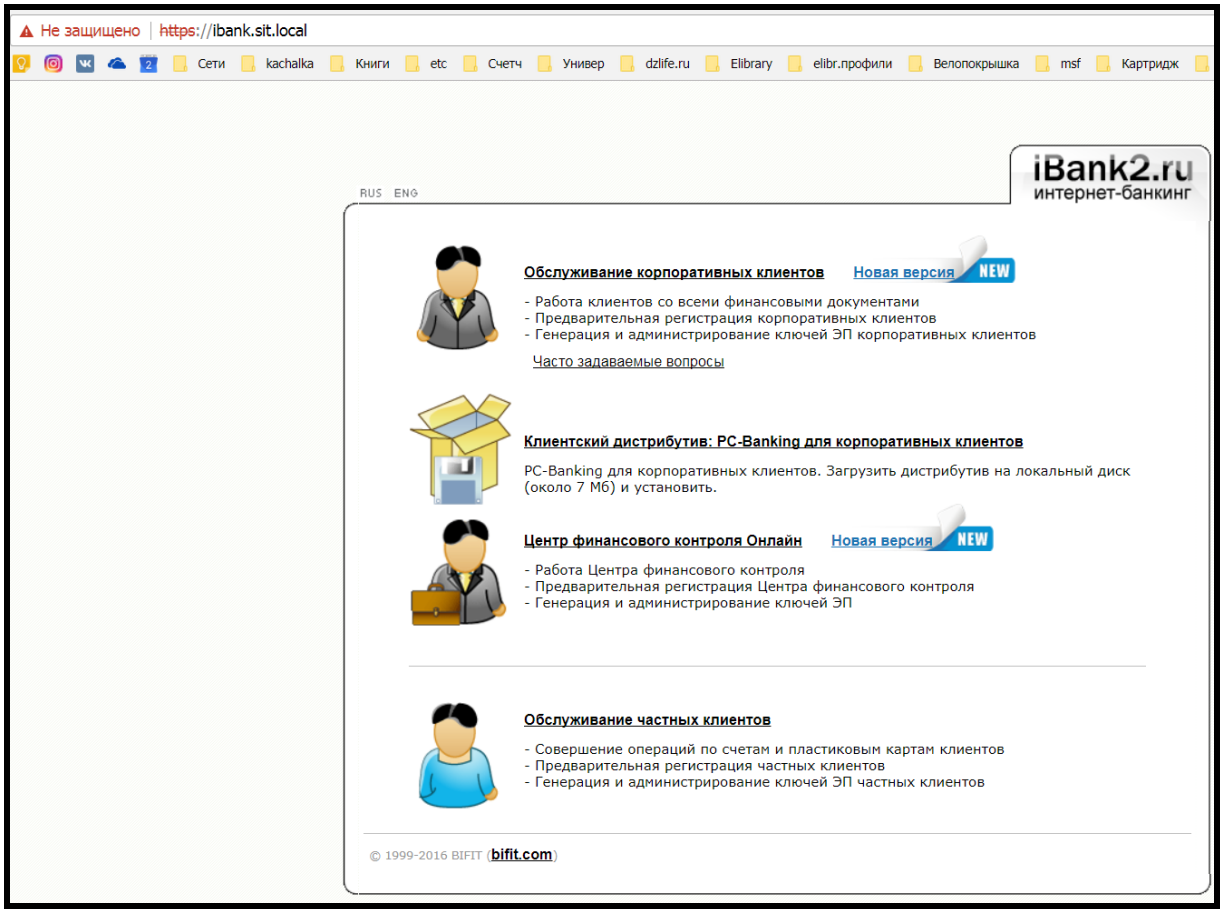

Рис. 2.3.1. Вход в систему

На странице выберите пункт Обслуживание корпоративных клиентов. Сначала загрузится стартовая html-страница, а через 15–30 с (в зависимости от скорости доступа к Интернету) загрузится АРМ. Окно «Вход в систему» предназначено для аутентификации пользователя (рис. 2.3.2, 2.3.3).

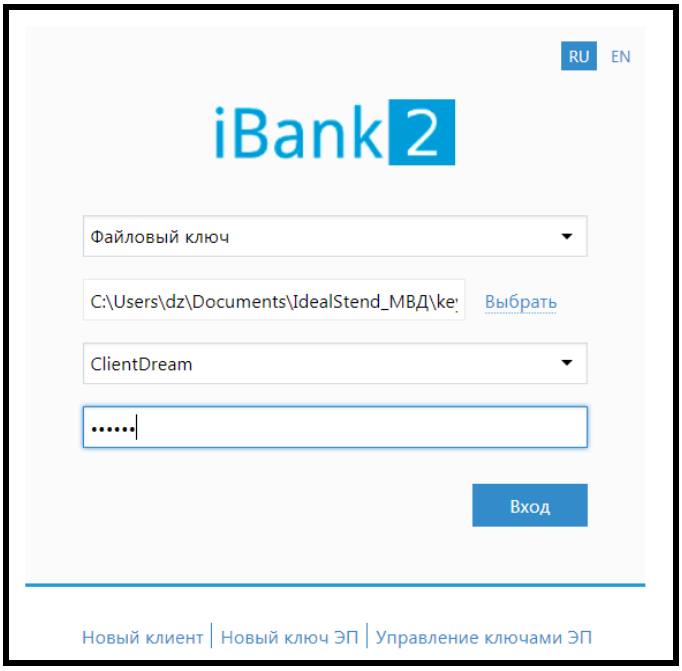

Рис. 2.3.2. Вход в систему

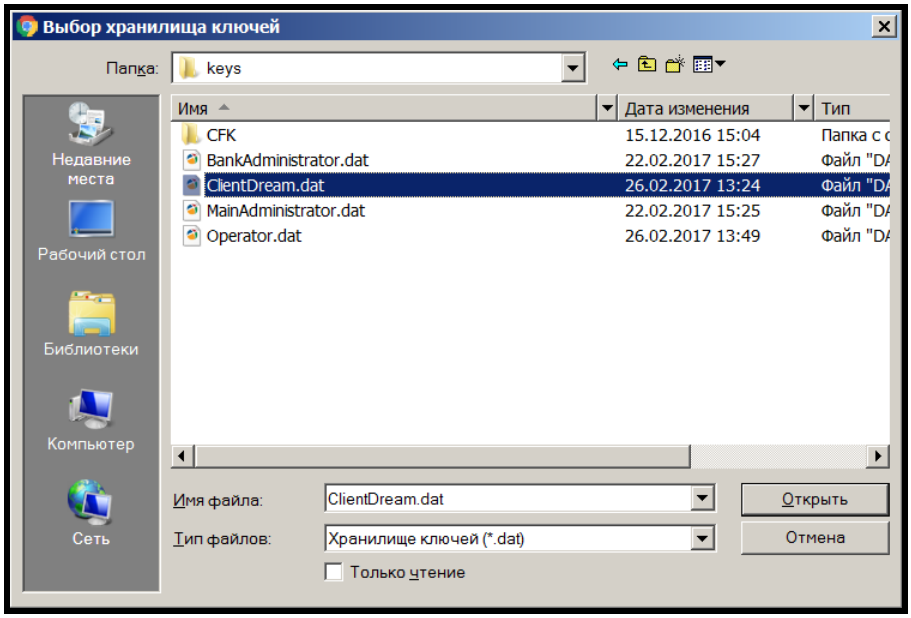

Рис. 2.3.3. Окно авторизации

В окне «Вход в систему» выполните:

Из списка поля «Тип хранилища» выберите тип хранилища «Файловый ключ». Для выбора ключа воспользуйтесь ссылкой «Обзор». Из списка поля «Ключ» выберите необходимый ключ ЭП и в соответствующее поле укажите пароль к нему. При вводе пароля учитываются язык (русский/латиница) и регистр (заглавные/прописные буквы). Пароль 123456. Нажмите кнопку «Вход». После успешной аутентификации на экран выводится стартовое окно АРМ «Internet-Банкинг для корпоративных клиентов», внешний вид которого представлен на рис. 2.3.4.

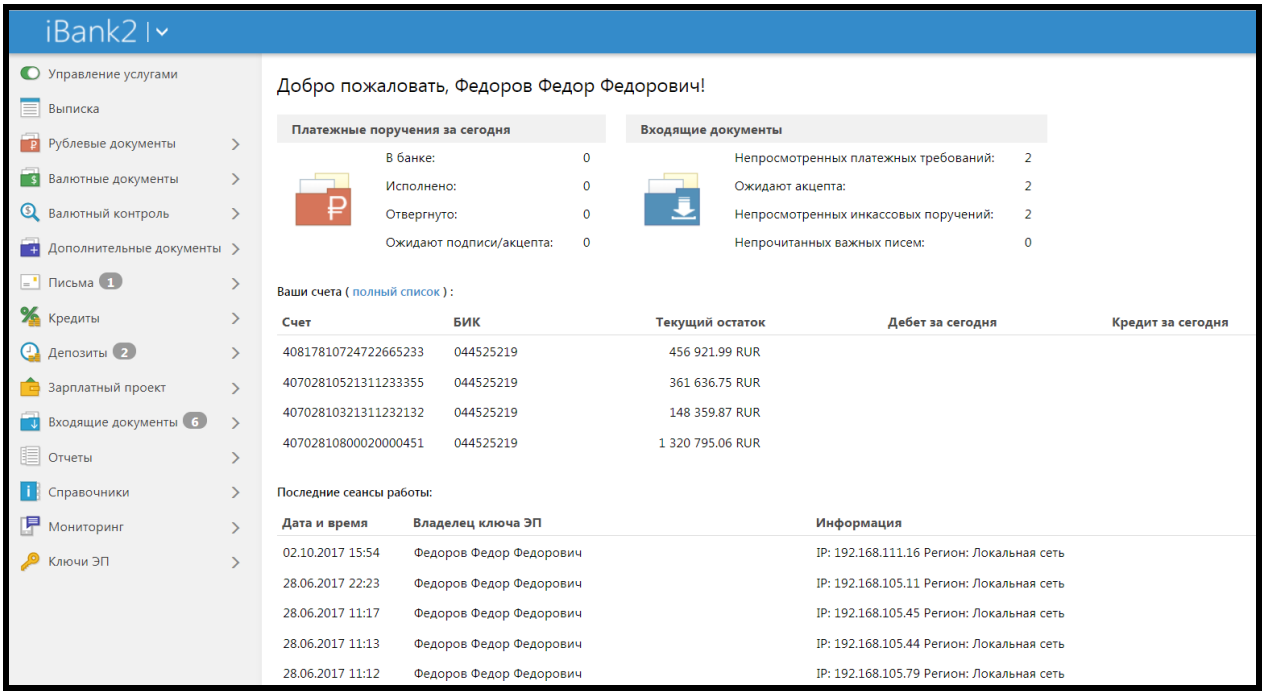

Рис. 2.3.4. «Internet-Банкинг для корпоративных клиентов». Стартовое окно

В данном окне показывается следующая информация:

– количество платежных поручений за сегодня. Документы разделены на категории в зависимости от статуса обработки;

– количество необработанных входящих документов. При наличии в системе непрочитанных важных писем работа в системе будет заблокирована до тех пор, пока клиент не ознакомится с ними.

Список всех счетов. Для переключения между кратким и полным списком используйте соответствующую ссылку рядом с заголовком таблицы.

Таблица, содержащая сведения о последних сеансах работы Вашей организации: дату и время сеанса; имя сотрудника – владельца ключа ЭП, с помощью которого был осуществлен вход в АРМ; информацию об устройстве и регионе подключения. Переход к данной таблице возможен также из раздела Сеансы работы дерева документов.

Интерфейс Internet-Банкинга. Главное окно

Вид главного окна АРМ «Internet-Банкинг для корпоративных клиентов» и его основные элементы представлены на рис. 2.3.5.

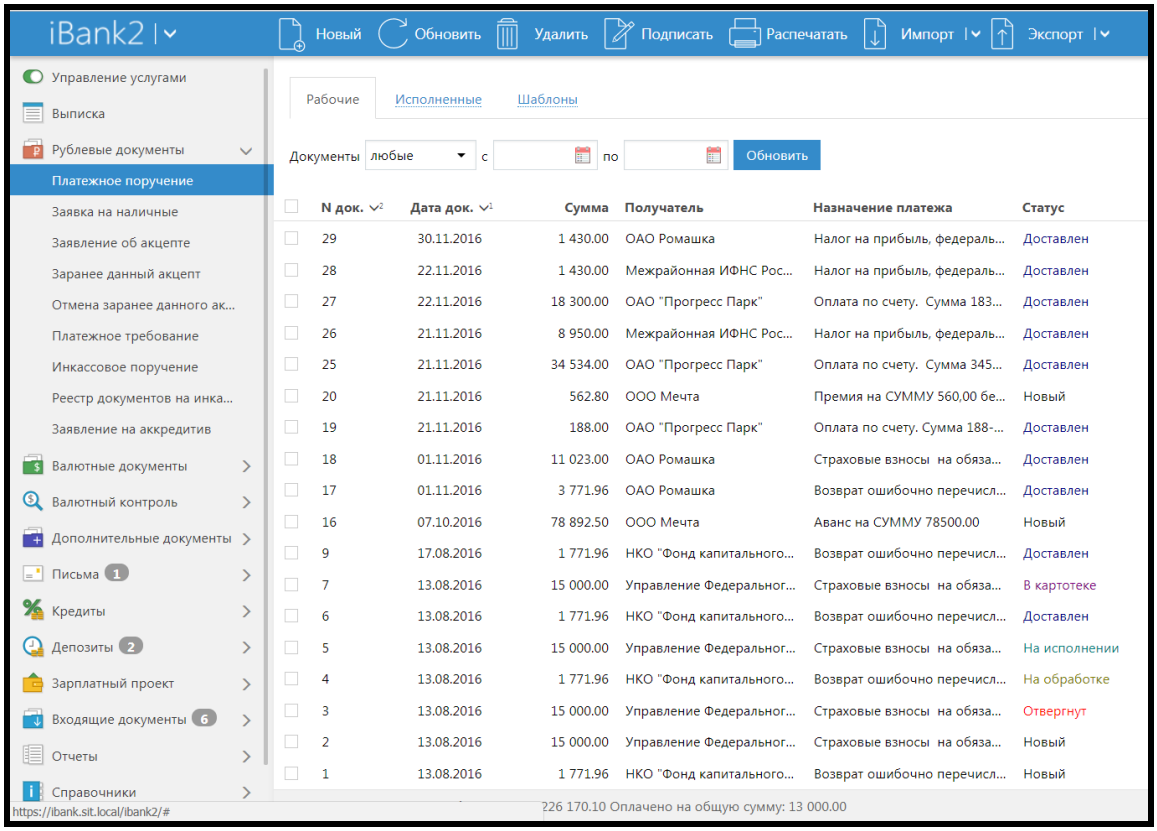

Рис. 2.3.5. «Internet-Банкинг для корпоративных клиентов». Элементы интерфейса

Входящие документы

В системе «iBank 2» предусмотрена возможность получение от банка входящих платежных требований и инкассовых поручений.

При наличии новых входящих документов Платежное требование или Инкассовое поручение, не просмотренных пользователем, раздел Входящие документы и соответствующий подраздел дерева документов будет выделен жирным шрифтом, а в скобках указано общее количество поступивших документов, рис. 2.3.6.

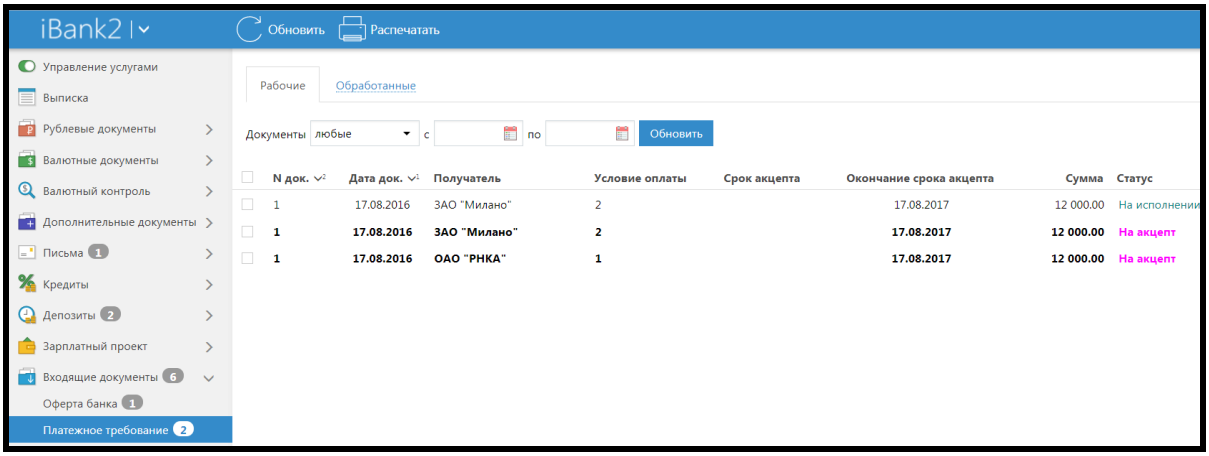

Рис. 2.3.6. Входящие документы. Платежное требование

Отчеты. Выписки

Выписка представляет собой перечень операций по выбранному счету с указанием списанных или зачисленных средств, номера платежного документа, на основании которого была проведена операция, и другой дополнительной информации, рис. 2.3.7.

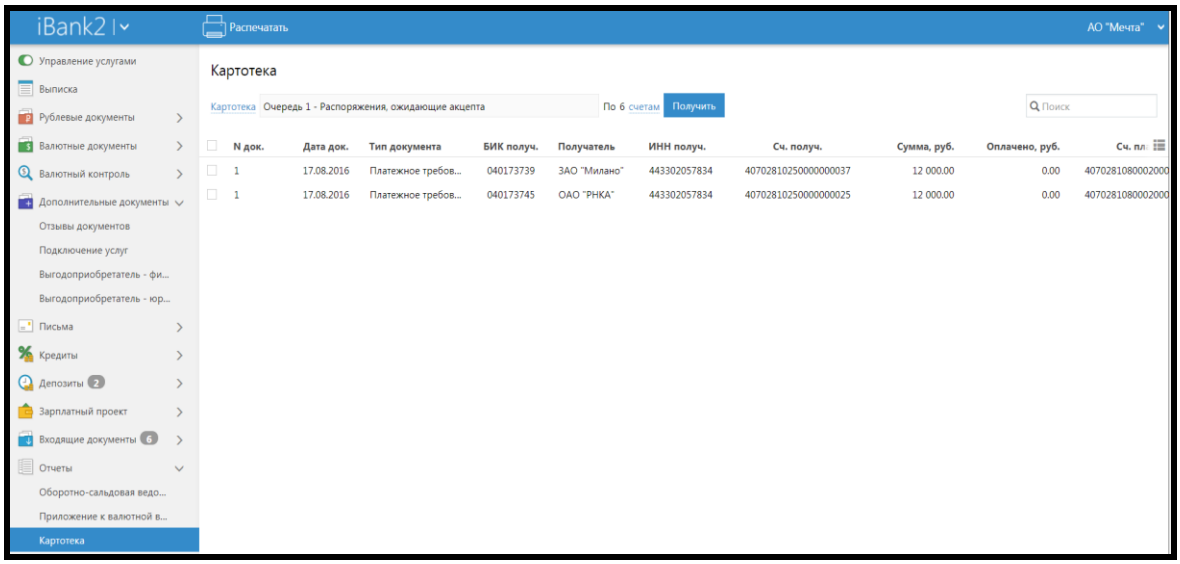

Рис. 2.3.7. Картотека

Для получения выписки по счету в дереве документов выберите категорию Выписки и выполните следующие действия:

– при необходимости измените предложенный системой банк (ссылка «Банк») или номер счета (ссылка «Счет»). Взаимосвязь типов документов и типов счетов подробно описана в пункте Использование типов счетов в документах раздела приложения;

– вручную или с помощью календаря дат задайте период выписки в полях *С* и *По*. Если поле с не заполнено, то началом периода выписки считается дата открытия счета; если не заполнено поле по, то окончанием периода выписки считается текущая дата. Если оба поля с и по оставить незаполненными, то выписка будет получена с даты открытия счета по текущую дату, рис. 2.3.8.

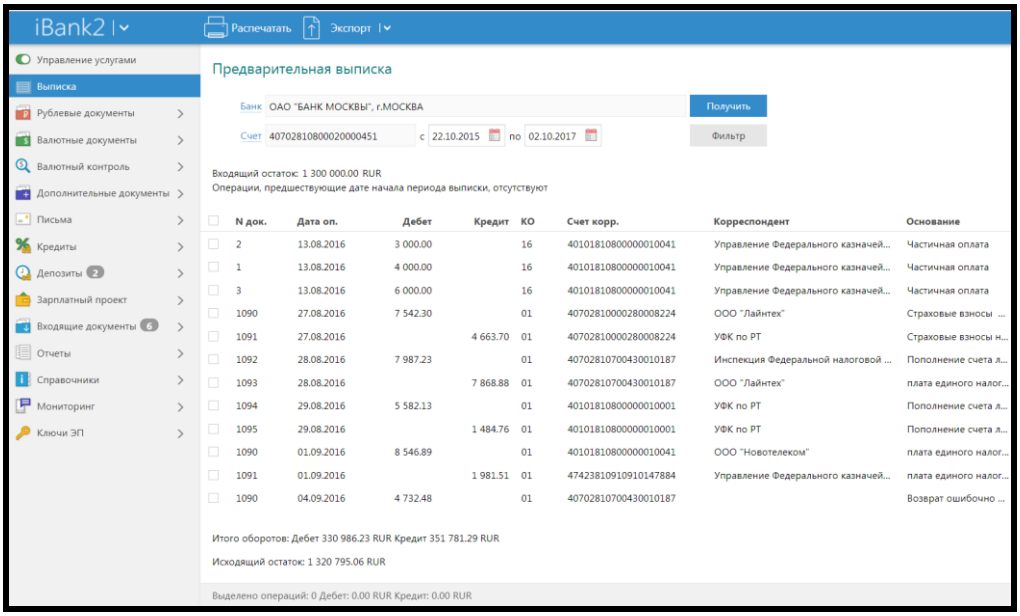

Рис. 2.3.8. Выписка по счету

Режим обслуживание частных клиентов

В окне выбора режимов работы необходимо нажать «Обслуживание частных клиентов» (рис. 2.3.9). Страница выбора режимов работы располагается по адресу URL: https://ibank.sit.local.

Авторизуемся с использованием учетных данных 123456 паролем 1234567.

На главной странице представлена краткая сводка по всем активам данной учетной записи, включая имеющиеся карты, шаблоны платежей, информация о последнем посещении (рис. 2.3.10).

При нажатии на ссылку «История входов» (рис. 2.3.11), открывается информация с историей сеансов работы пользователя.

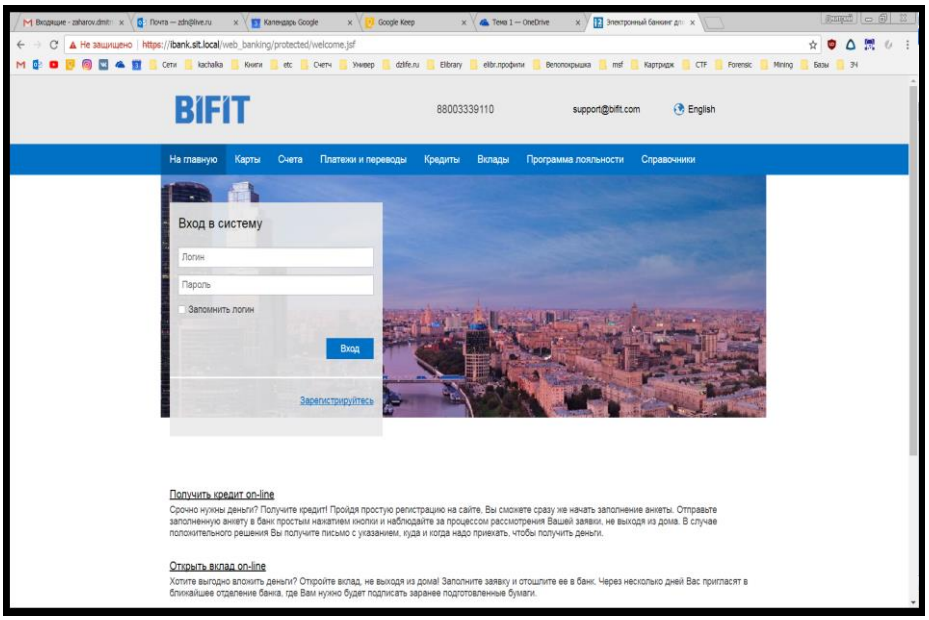

Рис. 2.3.9. Окно авторизации

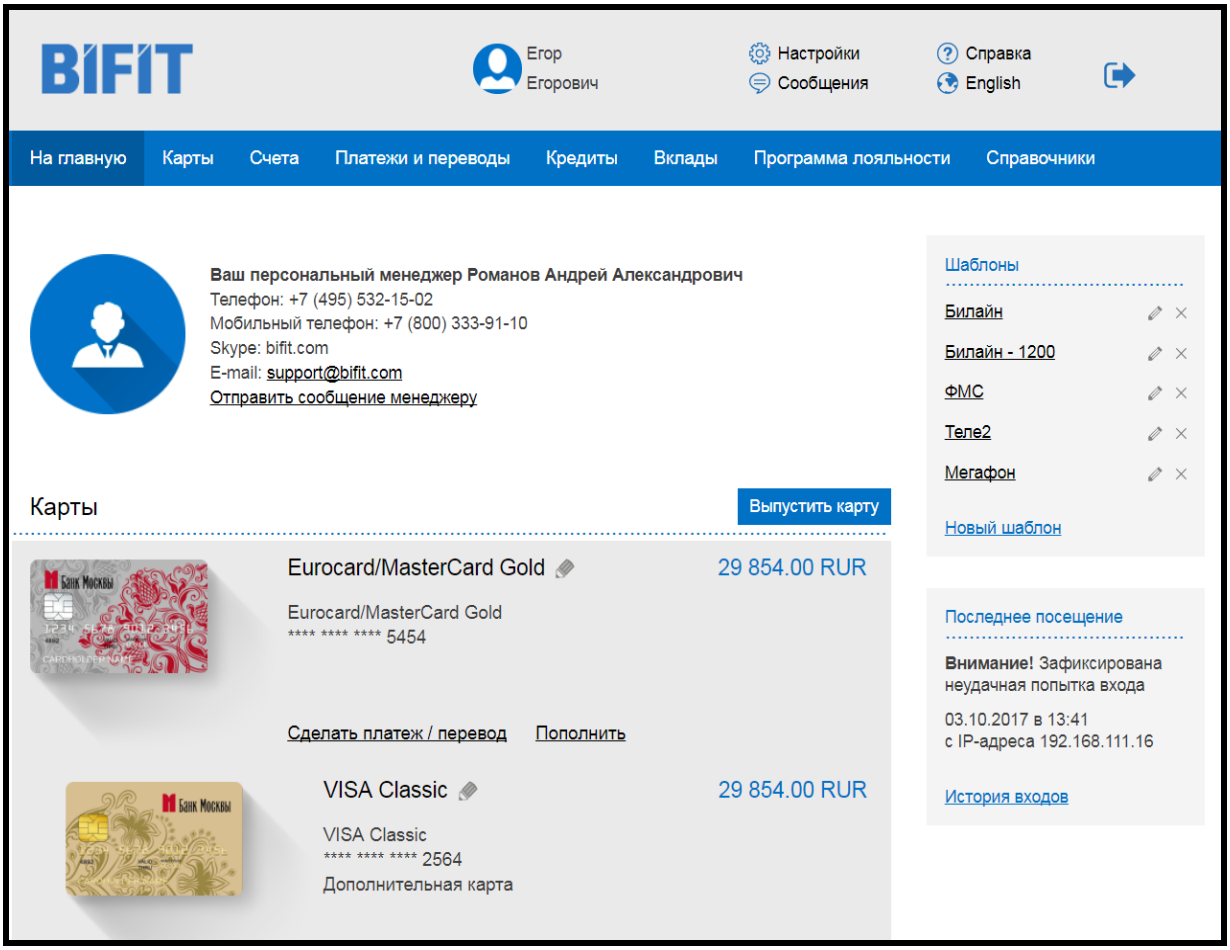

Рис. 2.3.10. Интерфейс

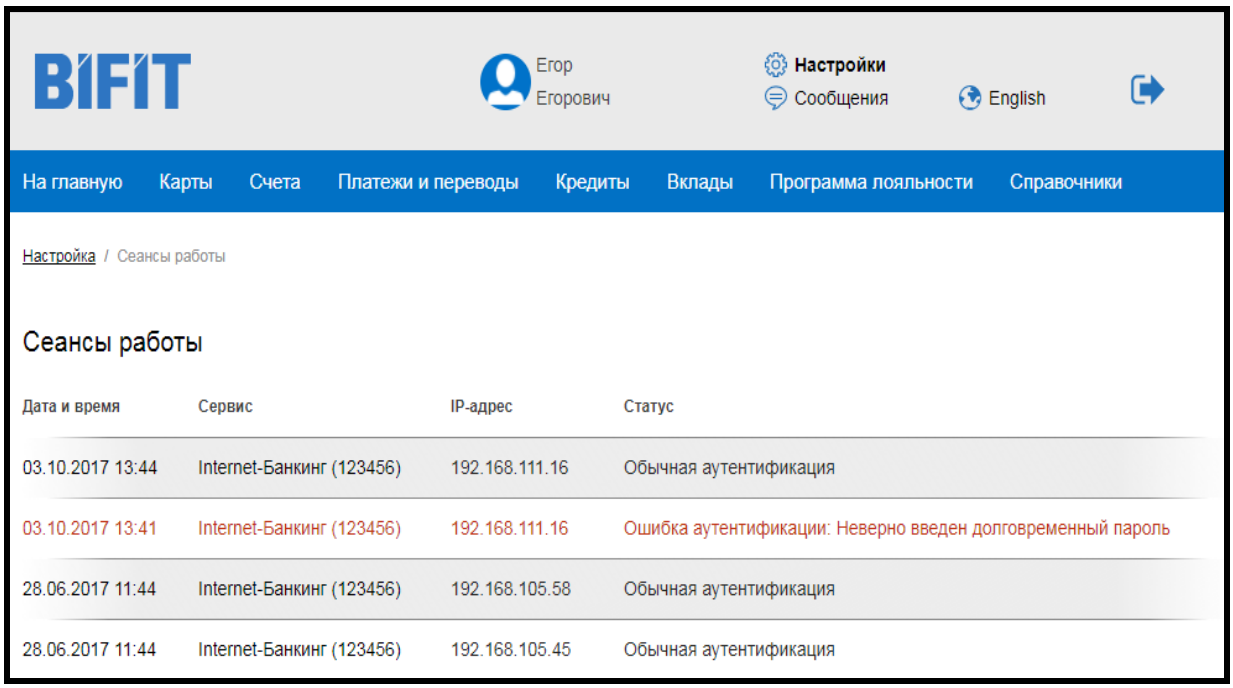

Рис. 2.3.11. Сеансы работы

Список карт пользователя

Для получения списка банковских карт пользователя необходимо зайти в меню «Карты» (рис. 2.3.12).

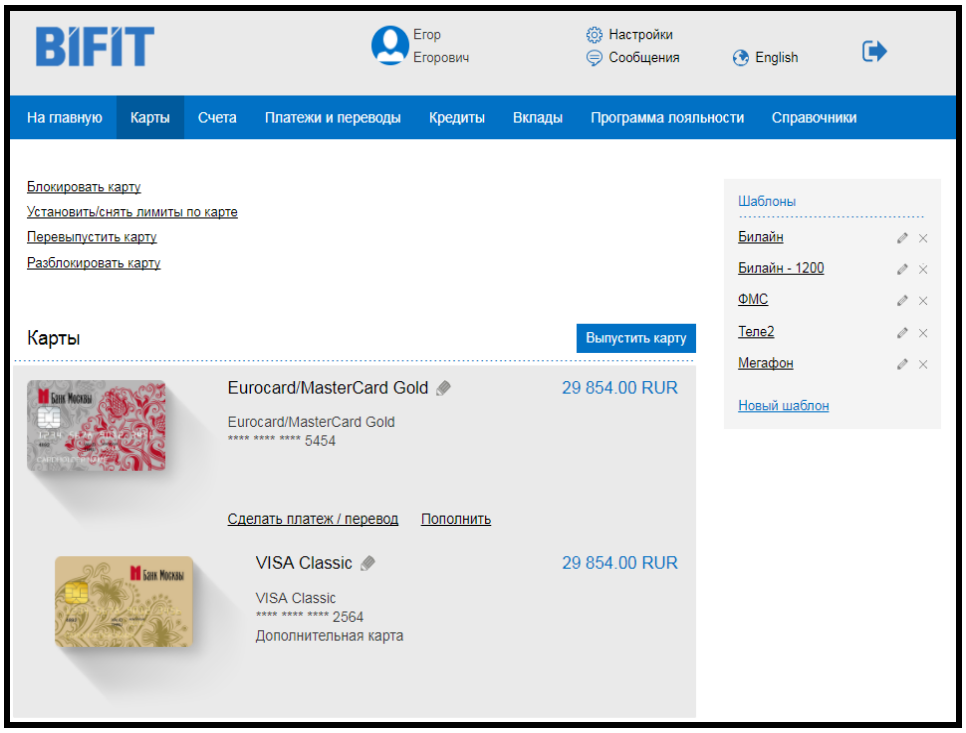

Рис. 2.3.12. Список карт пользователя

Для получения списка счетов пользователя необходимо зайти в меню «Счета» (рис. 2.3.13).

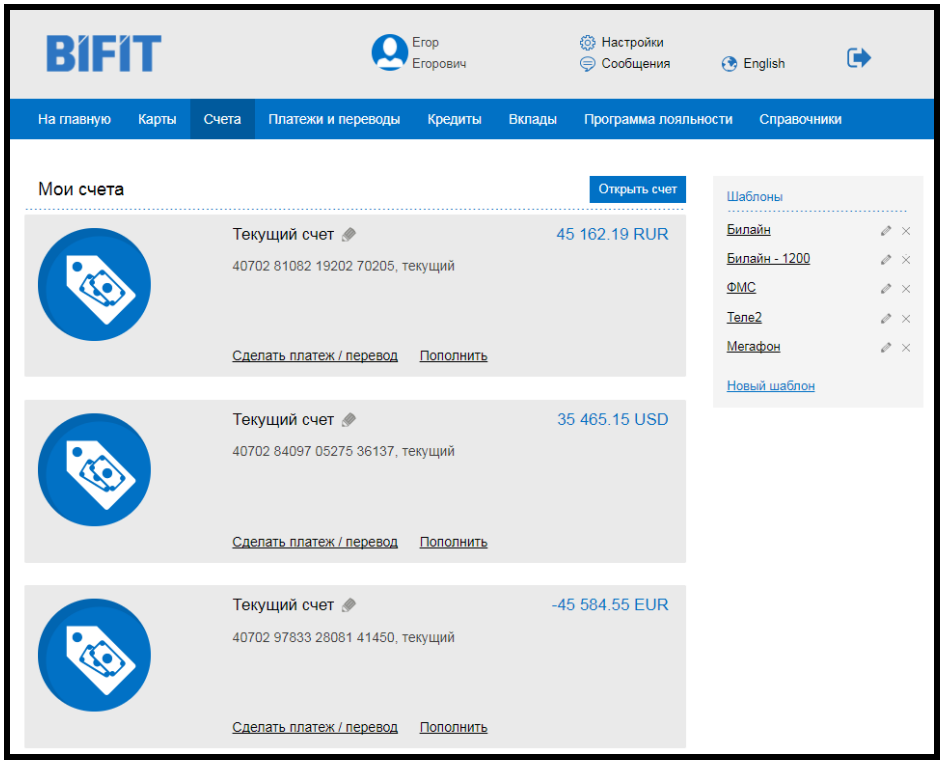

Рис. 2.3.13. Список счетов пользователя

Для получения детальной информации об операциях по каждому счету – необходимо зайти в него (рис. 2.3.14).

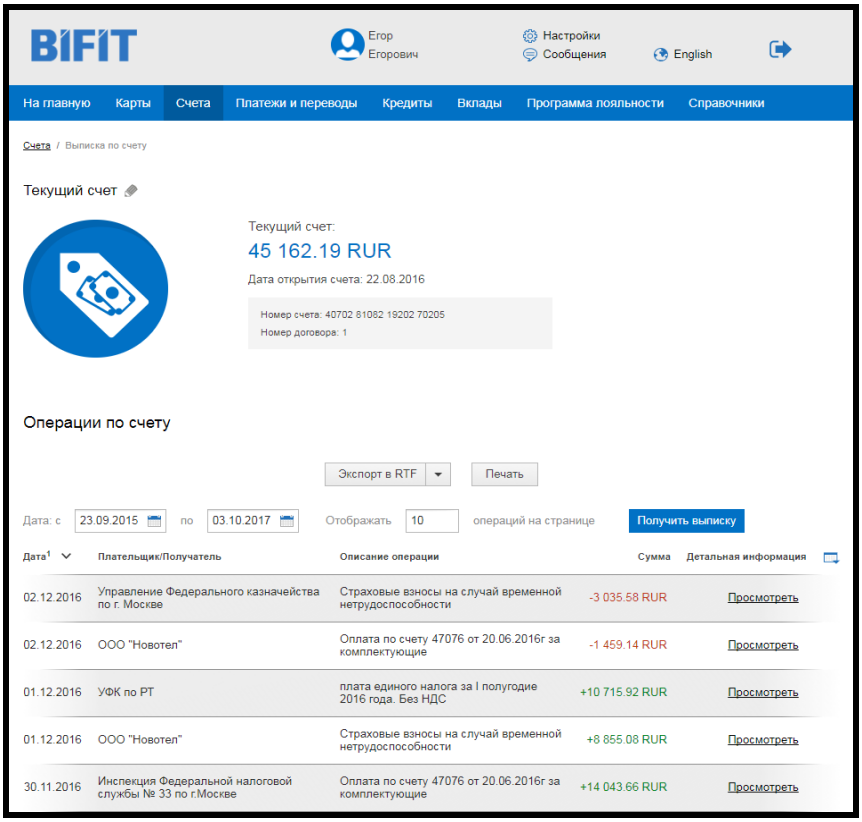

Рис. 2.3.14. Выписка по счету

Список вкладов пользователя

Для получения списка вкладов пользователя выберите пункт «Вклады» на главном меню (рис. 2.3.15).

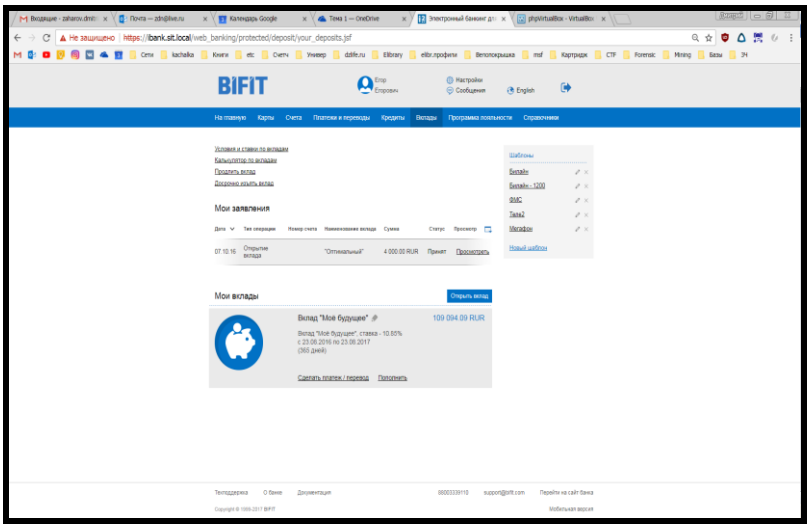

Рис. 2.3.15. Список вкладов пользователей

ГЛАВА III. ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ ПРОТИВ СОБСТВЕННОСТИ

§ 3.1. Сбор данных с устройств на базе ОС MS Windows

Действия при осмотре компьютера на базе ОС Windows. Проверка наличия активных сетевых подключений. Запуск командной строки. В среде MS Windows комбинация клавиш Win-R, затем команда cmd, затем – Enter (рис. 3.1.1).

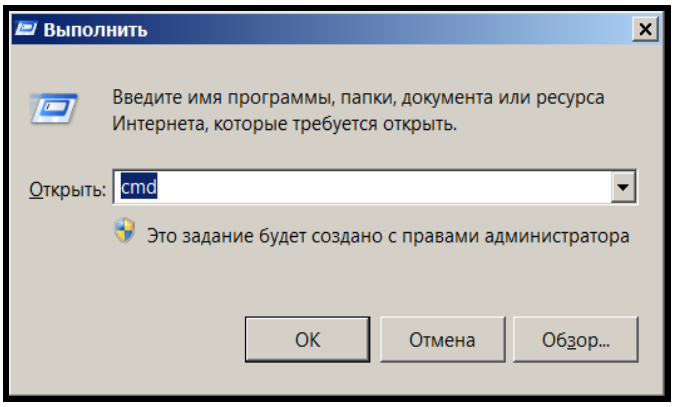

Рис. 3.1.1. Окно: Выполнить

В появившемся окне Обработчика команд Windows необходимо ввести команду: netstat –b > C:\connections.txt

Ключ –b переданный утилите netstat позволяет вывести названия исполняемых файлов, которые инициировали данное соединение.

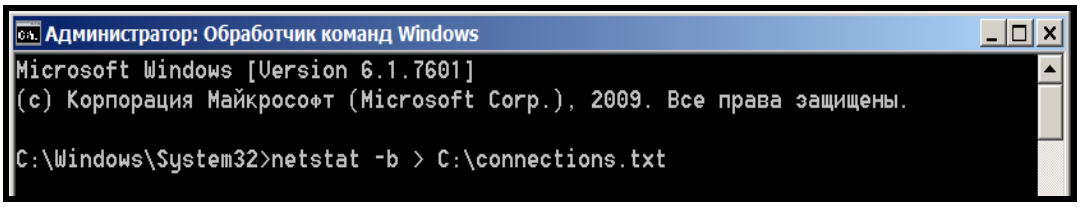

Рис. 3.1.2. Список активных соединений

В итоге вывод будет записан в файл, который был указан (рис. 3.1.2).

Вывод состоит из таблицы. В первом столбце название протокола. Во втором локальный адрес, в третьем столбце внешний адрес (с кем установлено соединение). **Список запущенных процессов и сервисов.** Оставаясь в том же окне командной строки, выполните команду (рис. 3.1.3): tasklist /SVC > tasklist.txt.

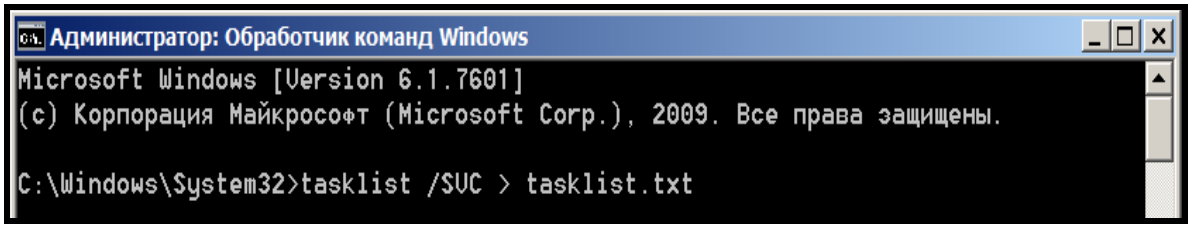

Рис. 3.1.3. Список процессов и сервисов

В итоге вывод будет записан в файл, который был указан. **Копирования кэша DNS.** Оставаясь в том же окне командной строки, выполните команду (рис. 3.1.4).

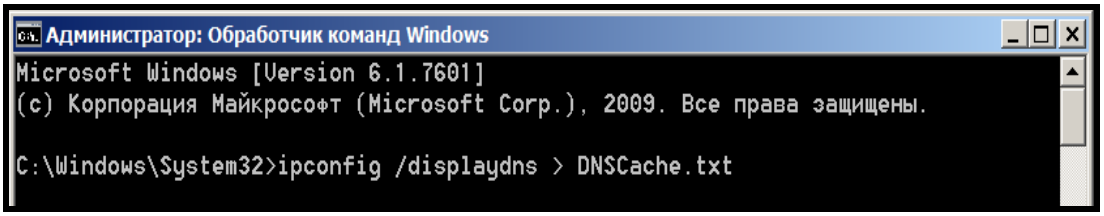

Рис. 3.1.4. Вывод кэша DNS

В итоге вывод будет записан в файл, который был указан. **Просмотр сетевых подключений.** В ОС MS Windows список активных сетевых интерфейсов можно просмотреть в Пуск->Панель управления->Сеть и интернет->Центр управления сетями и общим доступом->Изменение параметров адаптера (рис. 3.1.5). На данной странице будут перечислены все сетевые интерфейсы.

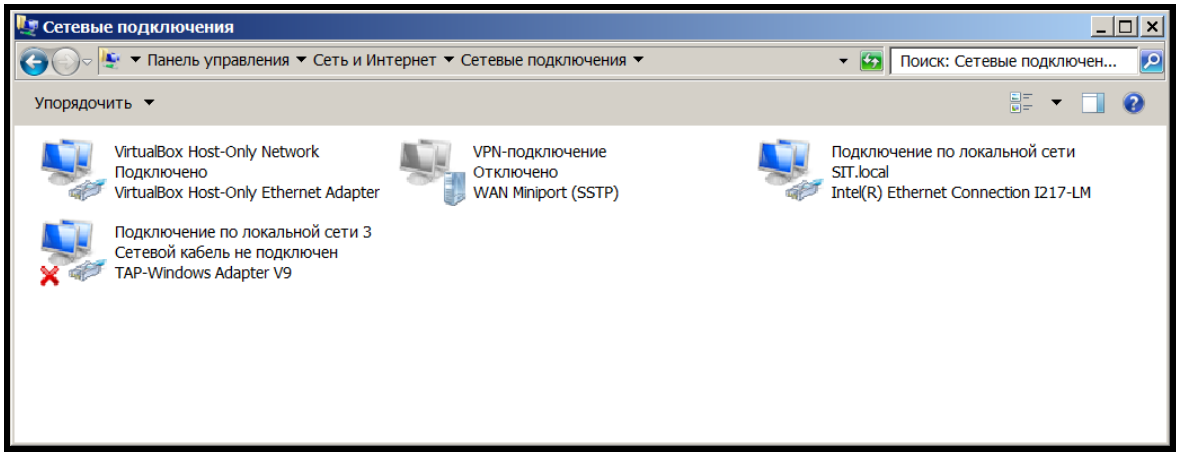

Рис. 3.1.5. Сетевые подключения

Напротив, отключенных сетевых интерфейсов, будет красный крест. Неактивные сетевые интерфейсы обозначены серым цветом и имеют статус «Отключено». У активных сетевых подключений будет статус «Подключено», либо название сети, к которой они подключены.

Просмотр состояния активных сетевых подключений выполняется путем щелчка ПКМ на требуемом сетевом подключении и выбором пункта Состояние (рис. 3.1.6).

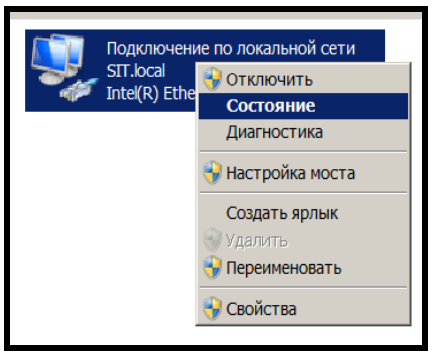

Рис. 3.1.6. Сетевое подключение

Будет показано окно «Состояние», в котором будет указана длительность подключения и объем переданных/полученных данных. Далее необходимо нажать кнопку «Сведения» (рис. 3.1.7). В появившемся окне будет приведена информация о текущем сетевом интерфейсе.

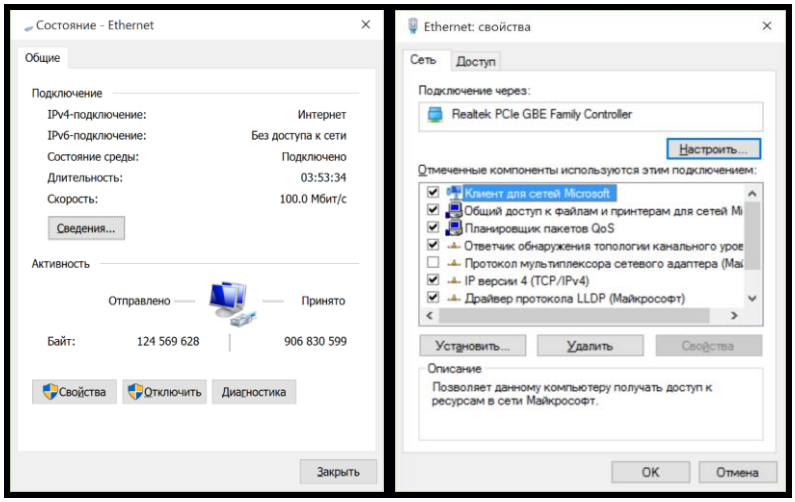

Рис. 3.1.7. Свойства сетевого адаптера

В окне сведения о сетевых подключениях (рис. 3.1.8), будет указана информация о текущем IP-адресе компьютера; о типе распределения адресов в данном сегменте исследуемой локальной сети; информация об IP-адресах DHCP-, DNS-серверов.

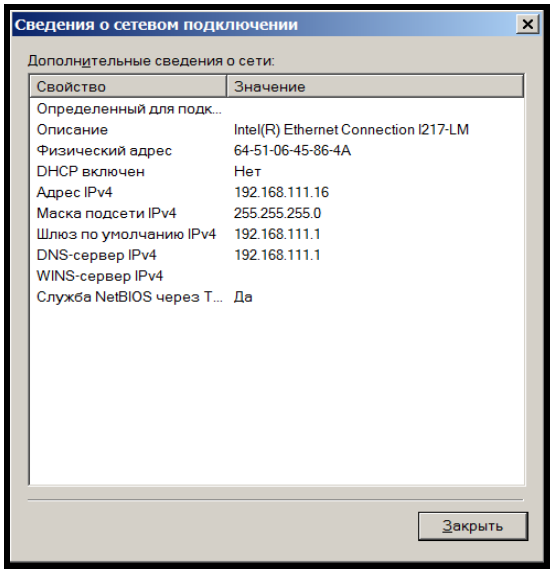

Рис. 3.1.8. Свойства сетевого подключения

Определение конфигурации протокола TCP/IP

В окне конфигурации сети выберите «IP версии 4 (TCP/IPv4)» и нажмите кнопку «Свойства». Откроется окно настройки параметров протокола TCP/IP. В данном окне откройте закладку IP-адрес. В данном окне может отсутствовать какая-либо информация о текущих настройках протокола, это свидетельствует о том, что установлен режим автоматического получения сетевых настроек с DHCP-сервера (рис. 3.1.9).

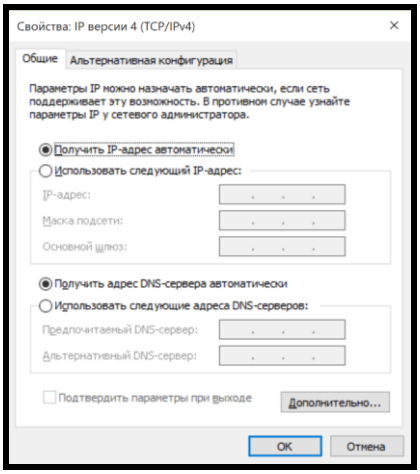

Рис. 3.1.9. Свойства IPv4

Для просмотра текущей конфигурации протокола TCP/IP воспользуйтесь программой ipconfig, входящей в состав операционной системы Windows. Программа является консольной, поэтому для ее выполнения необходимо запустить командую строку. Для этого нажмите кнопку «Пуск», в поле для поиска введите cmd и нажмите клавишу Enter. Вызовите программу ipconfig передав ей ключ /all (рис. 3.1.10).

Анализ маски подсети позволяет оценить размеры данного сегмента сети – так как маска 255.255.255.0, значит в IP-адресе первые три числа (192.168.105.) определяют адрес подсети, а последнее число (например, 10) – адрес компьютера в данной подсети. Следовательно, в данном сегменте сети может быть не более 254 компьютеров с адресами 192.168.105.1 … 192.168.105.254.

С уверенностью можно сказать о существовании двух компьютеров – данного компьютера (на рисунке имеет адрес 192.168.105.10) и основного шлюза с адресом 192.168.105.200.

Логически сеть состоит как минимум из двух сегментов: один из них – это сеть с адресами 192.168.105.xxx, в которой расположен данный компьютер, второй сегмент – сеть с адресами 192.168.1.xxx, в которой расположен компьютер с адресом 192.168.1.1, совмещающий в себе функции DNS-, DHCP- и WINS-сервера.

Рис. 3.1.10. Ipconfig

На экране отобразится окно, в котором выведены все настройки протокола IP.

Данная информация позволяет сделать ряд выводов:

В данной локальной сети используется динамическая система распределения адресов, адрес получен с сервера DHCP, имеющего адрес 192.168.1.1.

Отключение сетевых подключений

Производится путем извлечения сетевых кабелей с интерфейсом RJ-45 из порта сетевого адаптера (рис. 3.1.11, 3.1.12). В случае обнаружения беспроводных сетевых интерфейсов. Они могут быть выполнены в форме USB-флешки и могут быть вставлены в USB-порты компьютера спереди или сзади. Необходимо их извлечь. В случае обнаружения антенн в задней части системного блока – необходимо открутить эти антенны либо отключить сетевой интерфейс в панели управления (рис. 3.1.13).

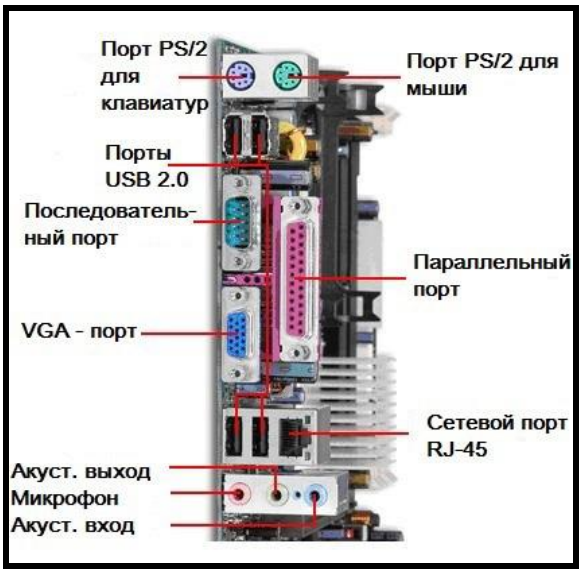

Рис. 3.1.11. Порты материнской платы

Рис. 3.1.12. Сетевой кабель

Рис. 3.1.1.13. PCI-Wi-fi адаптер

Получение снимка оперативной памяти

Снимок оперативной памяти так же создается с помощью утилит, например, FTK Imager.

Порядок действий:

Программный продукт FTK Imager предварительно записывается на сменный носитель.

Сменный носитель, содержащий FTK Imager необходимо подключить к ЭВМ, чей образ НЖМД требуется скопировать.

Далее подключается сменный носитель информации, на который будет скопирован образ.

Запускается файл «FTK Imager.exe» с правами администратора.

После загрузки появляется главное окно (рис. 3.1.14).

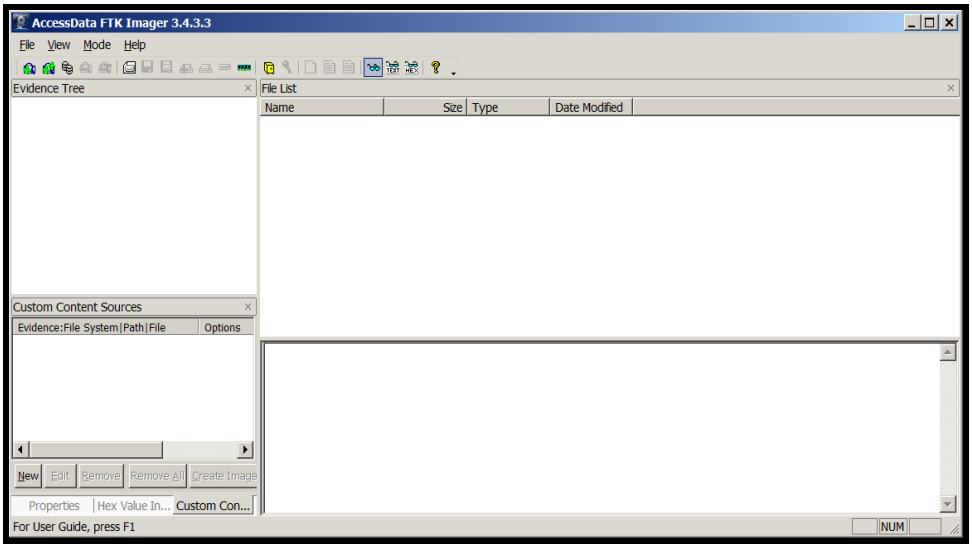

Рис. 3.1.14. Главное окно FTK Imager

Выбирается пункт меню File->Capture Memory (рис. 3.1.15).

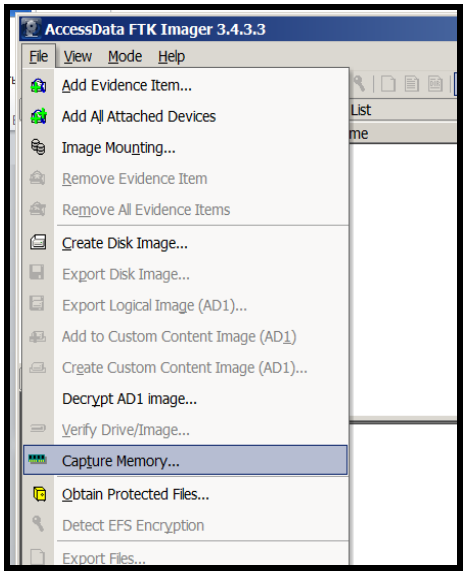

Рис. 3.1.15. Снимок оперативной памяти

Необходимо указать целевое устройство, куда будет сохранен снимок, путем нажатия кнопки Browse (рис. 3.1.16, 3.1.17).

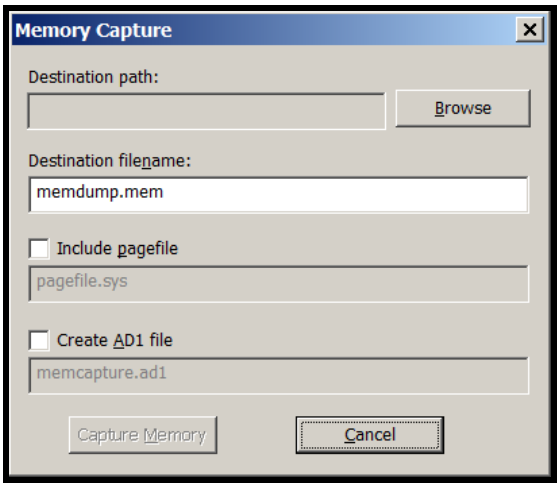

Рис. 3.1.16. Настройки снимка

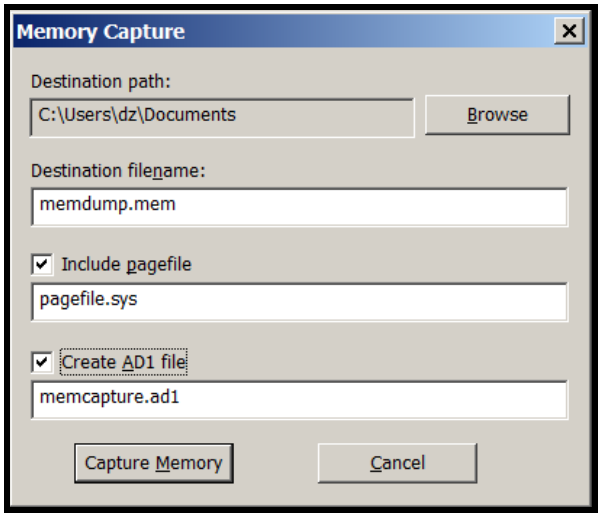

Рис. 3.1.17. Настройки снимка

Также необходимо отметить галками Include PageFile и Create AD1 file. После этого необходимо нажать кнопку Capture Memory. В результате в выходной папке окажутся необходимые снимки.

Получение снимка содержимого жесткого диска

Снимок жесткого диска создается с помощью специальных утилит. Они в большинстве бесплатны. Например, FTK Imager.

Первоначальный порядок действий схож со снятием снимка оперативной памяти. После загрузки появляется главное окно.

Выбирается пункт меню «File – Create Disk Image...». Будет отображено окно выбора типа источника данных (рис. 3.1.18).

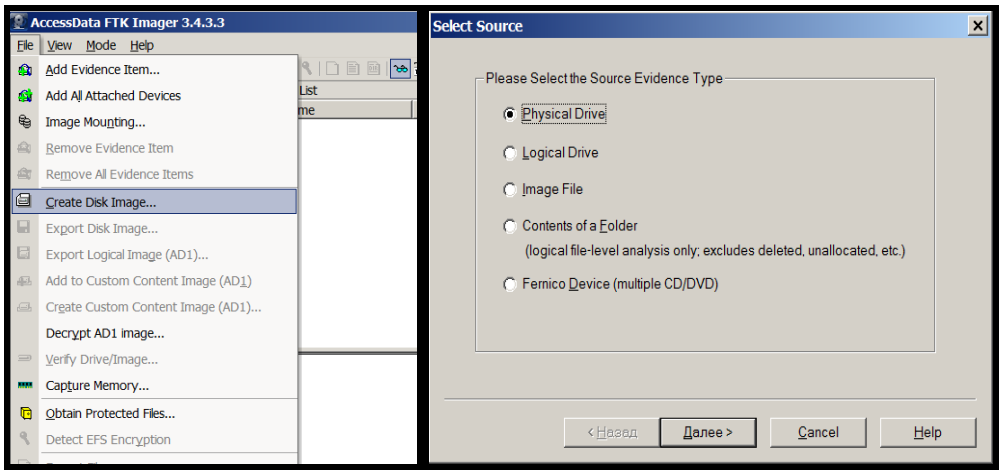

Рис. 3.1.18. Создание образа

В качестве типа источника чаще всего используется «Физический диск». Выбор «Логический диск» рекомендуется в следующих случаях:

– носители информации в ЭВМ образуют программный отказоустойчивый массив (RAID), а данные следует скопировать в декодированном виде (для исключения дальнейшей сборки массива);

– используется программное шифрование всего содержимого носителей информации в ЭВМ (полнодисковое шифрование), а данные следует скопировать в расшифрованном виде.

Далее необходимо выбрать источник данных (рис. 3.1.19).

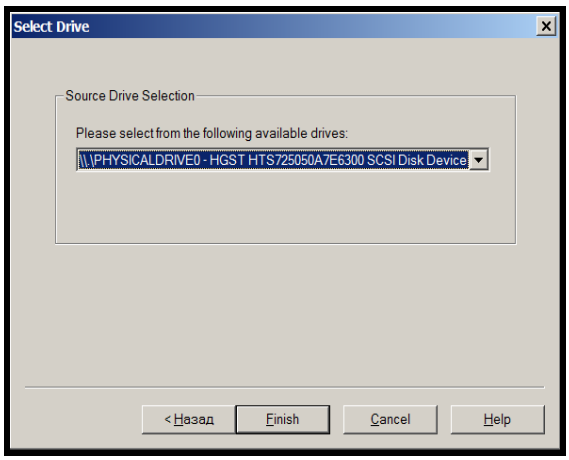

Рис. 3.1.19. Устройство – источник

Отображается общее окно параметров создаваемых образов. В указанном окне следует нажать кнопку «Add...» (рис. 3.1.20).

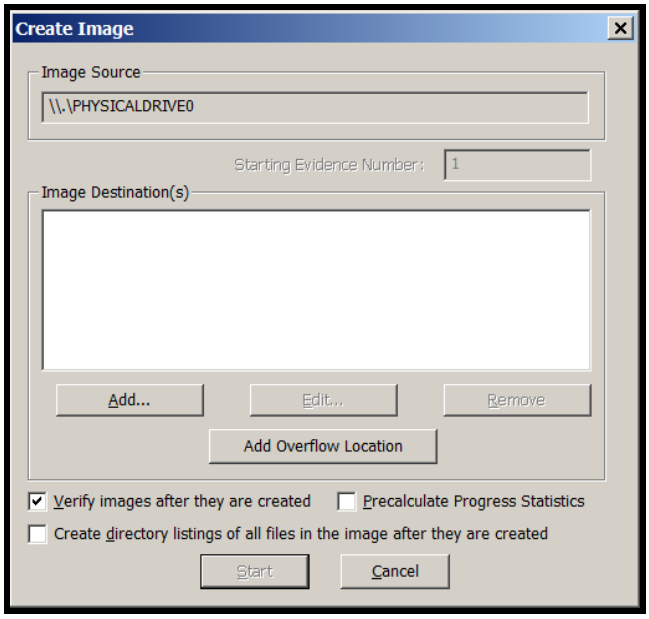

Рис. 3.1.20. Создание образа

Отображается окно выбора типа создаваемого образа. В указанном окне рекомендуется выбрать «Raw (dd)» – точная копия данных без сжатия или шифрования (рис. 3.1.21).

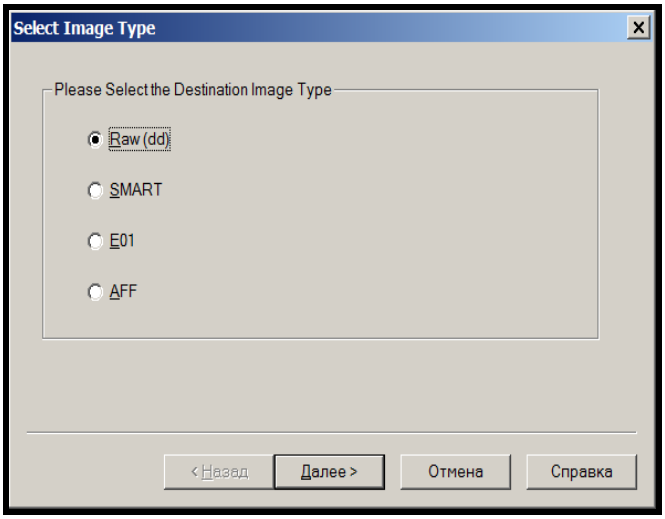

Рис. 3.1.21. Выбор типа образа

Окно ввода дополнительной информации не является обязательным к заполнению. Рекомендуется ввести фамилию человека, создающего образ (поле «Examiner»), и сведения, указывающие на ЭВМ, образы носителей информации, с помощью которой создается поле «Notes» (рис. 3.1.22).

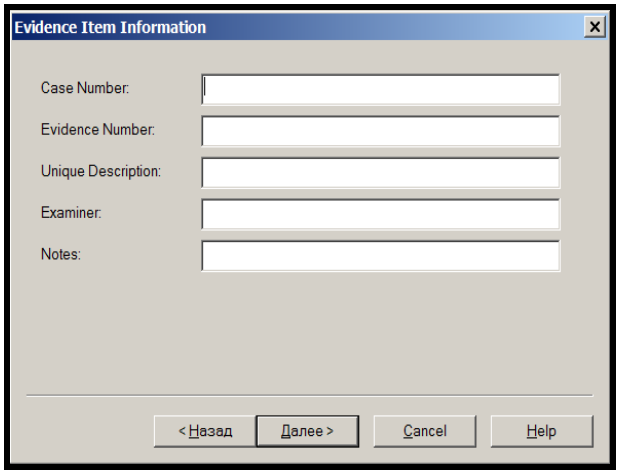

Рис. 3.1.22. Ввод дополнительной информации

Будет запущен процесс копирования данных, состояние которого отображается в статусном окне. После завершения копирования в поле «Status» будет отображена строка «Image created successfully» (рис. 3.1.33).

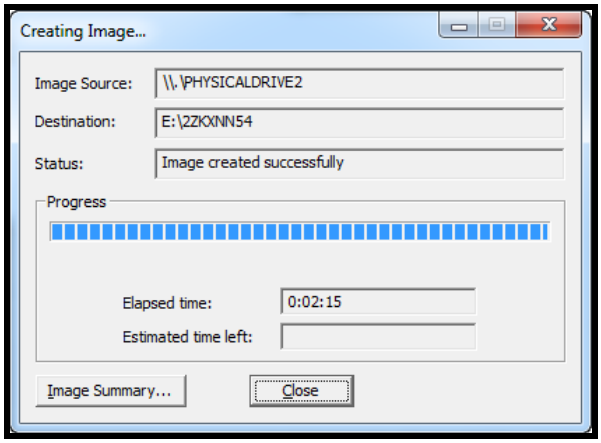

Рис. 3.1.33. Создание образа

В результате в директории, выбранной для сохранения создаваемого образа, будут записаны два файла: файл-образ и текстовый файл, содержащий дополнительную информацию (рис. 3.1.34).

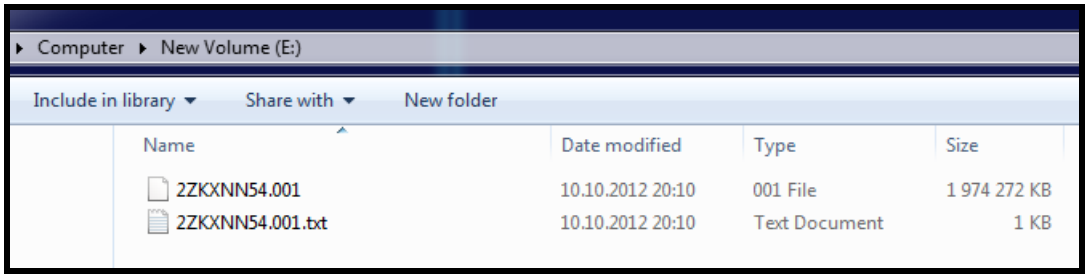

Рис. 3.1.34. Выходные файлы

Поиск информации на ОС Windows

Выполните характеристику все доступные на вашем компьютере носители информации. Откройте Проводник->«Мой компьютер» и перечислите все устройства и диски, подключенные к компьютеру (рис. 3.1.35).

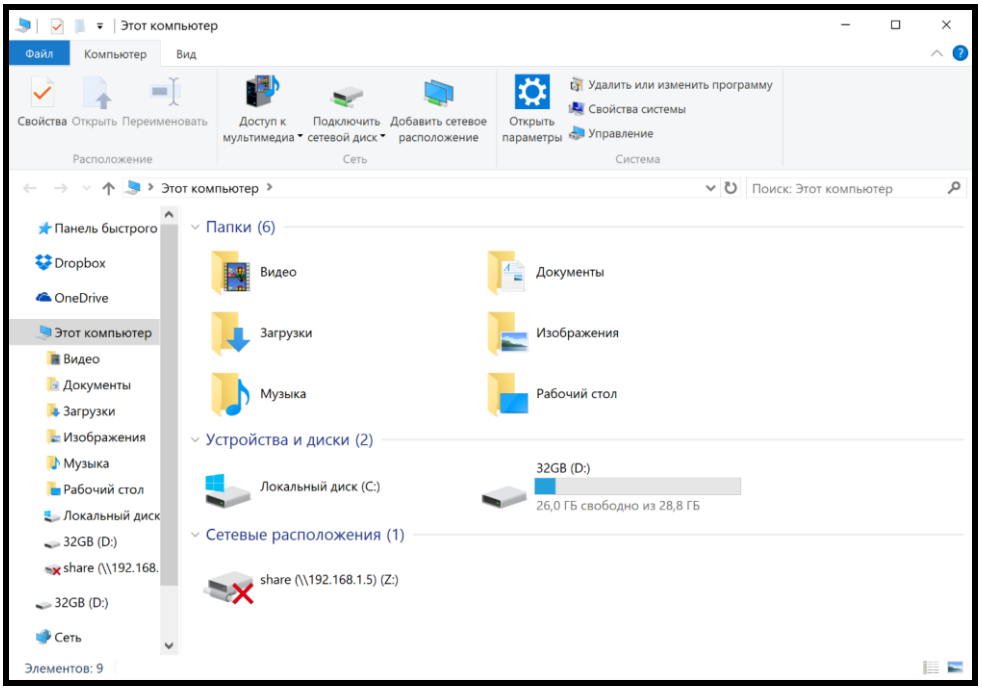

Рис. 3.1.35. «Мой компьютер»

Ознакомьтесь с устройствами и проведите классификацию, в соответствии с материалами лекции (по назначению, по устойчивости записи, по энергозависимости, размеру и т. д.).

Консоль «Управление дисками»

Изучите основные возможности стандартной консоли управления дисками (рис. 3.1.36, 3.1.37).

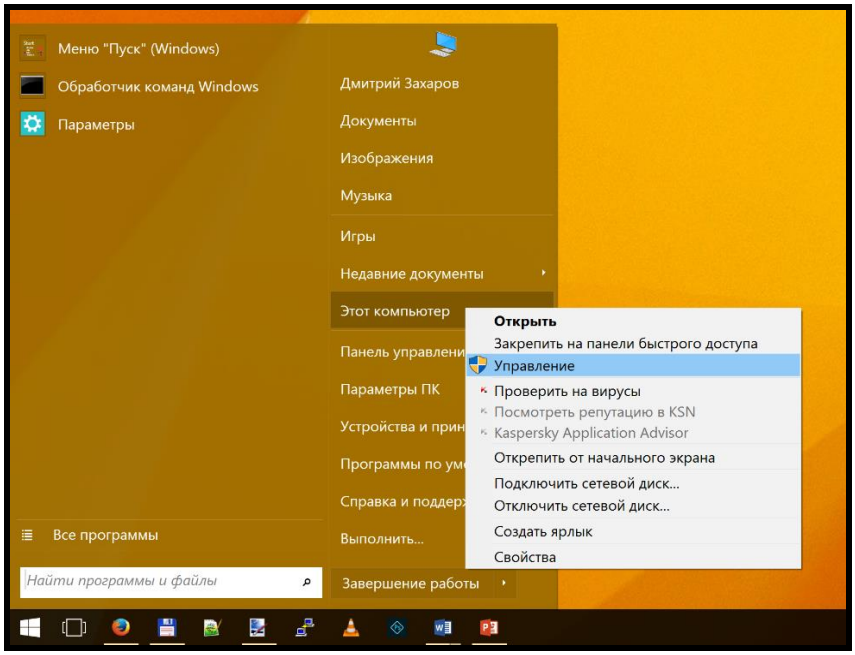

Рис. 3.1.36. Запуск консоли управления дисками

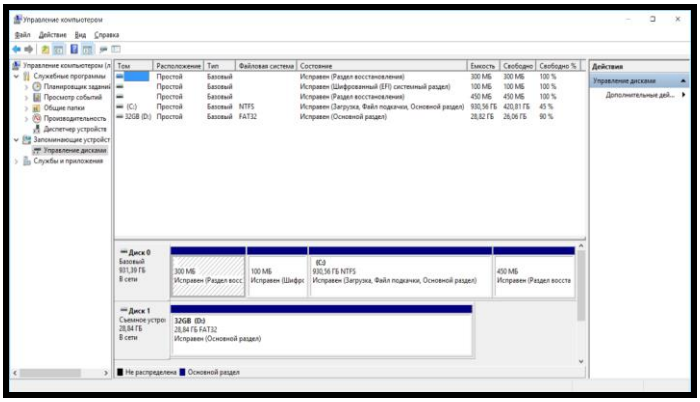

Рис. 3.1.37. Консоль управления дисками

Выясните количество разделов на жестком диске и количество физических жестких дисков.

Перечислите характеристики разделов (тип файловой системы, размер, в каком месте диска они находятся, букву).

Выясните стиль таблицы разделов. Правым кликом мыши на диске выберите пункт «Свойства» (рис. 3.1.38).

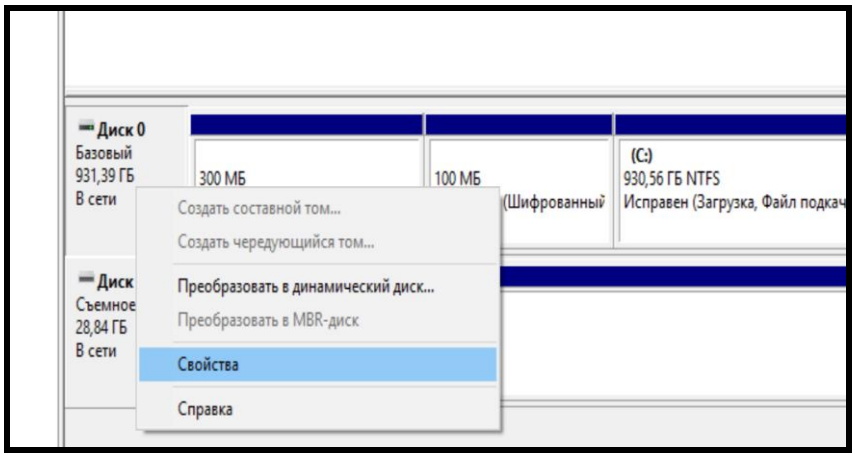

Рис. 3.1.38. Свойства жесткого диска

Откроется окно свойств (рис. 3.1.39).

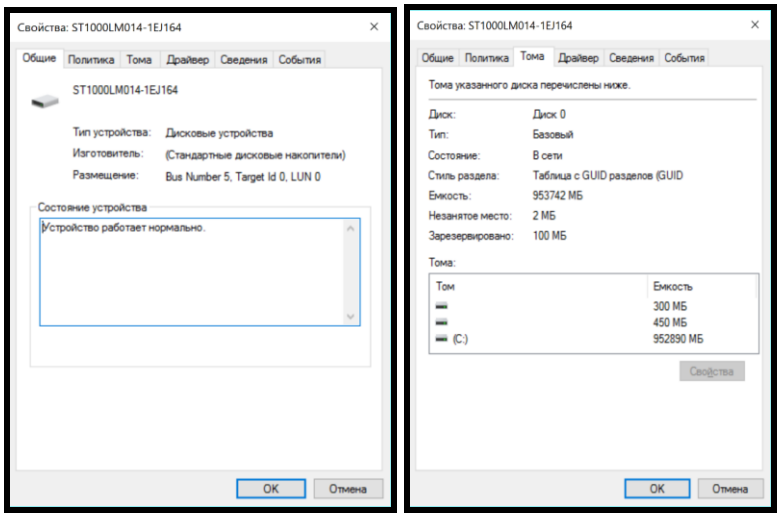

Рис. 3.1.39. Свойства жесткого диска

Находясь на вкладке «Общие» – запишите модель устройства, тип устройства и его состояние. Перейдите на вкладку «Тома» и перечислите все разделы (также их называют томами), которые есть на жестком диске. Отдельно обозначьте те, которые не имеют буквы. Выясните стиль таблицы разделов на носителе.

Исследование скрытых разделов жесткого диска

Стандартная консоль управления дисками не позволяет назначить букву скрытым системным разделам. Для того чтобы исследовать, скажем раздел восстановления, необходимо его смонтировать в системе. В терминологии Windows – назначить ему букву. Для того чтобы это сделать воспользуемся встроенной утилитой diskpart. Запустите diskpart. Для этого нажмите ПУСК и наберите diskpart.

Запуститься консоль Windows и утилита diskpart (рис. 3.1.40).

Следующим шагом необходимо выяснить номера разделов и имеющееся у них имя. Для этого выполним команду list volume в окне diskpart (рис. 3.1.41). У нас имеются несколько разделов без букв. Выберем первый, который не имеет буквы. В данном случае это «Том 1», 1 означает номер раздела (в вашем случаем это может быть другой том).

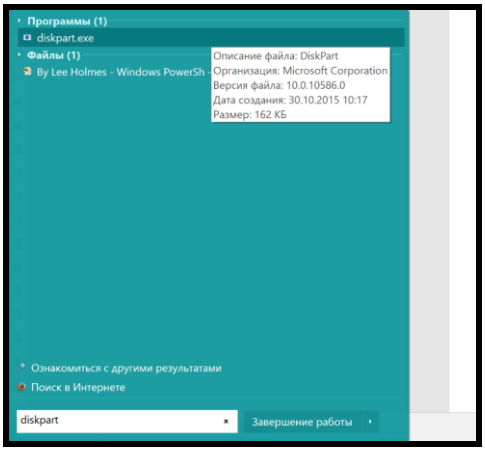

Рис. 3.1.40. Запуск diskpart

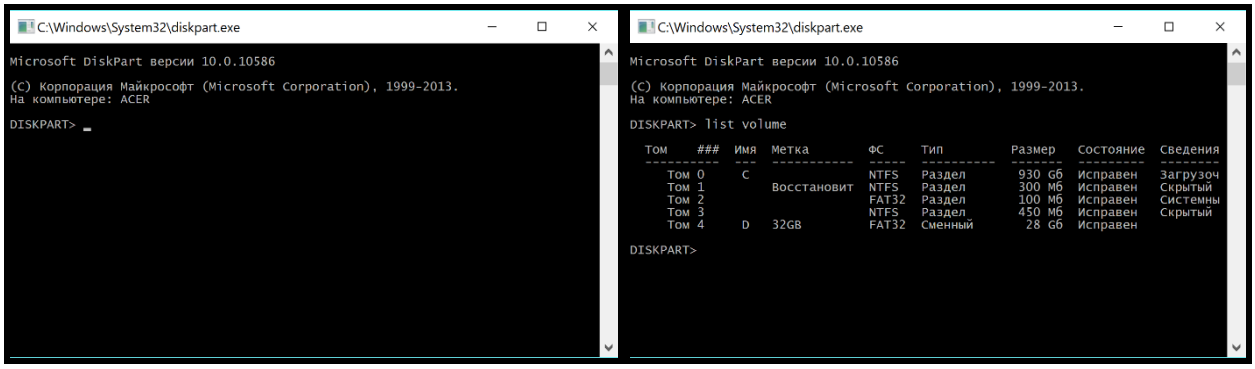

Рис. 3.1.41. Утилита diskpart

Необходимо выбрать соответствующий том, для этого выполним команду: select volume <номер тома>.

В данном случае команда будет: select volume 1 (рис. 3.1.42).

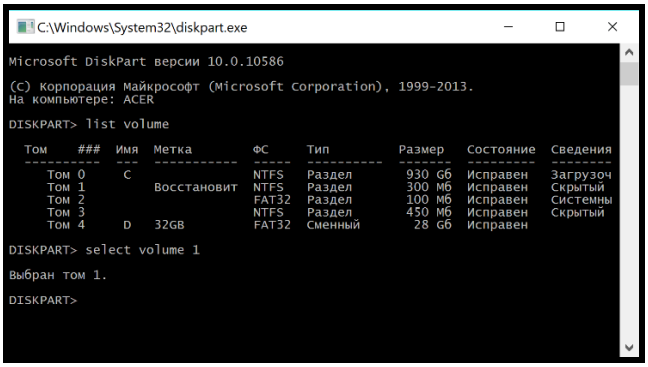

Рис. 3.1.42. Выбран том

Далее необходимо присвоить букву разделу. Воспользуйтесь списком, который вы создали и выясните какие буквы заняты. Выберете любую свободную, в данном случае E. Выполним команду присваивания буквы разделу: assign letter=<буква>.

В данном случае команда будет выглядеть: assign letter=E (рис. 3.1.43).

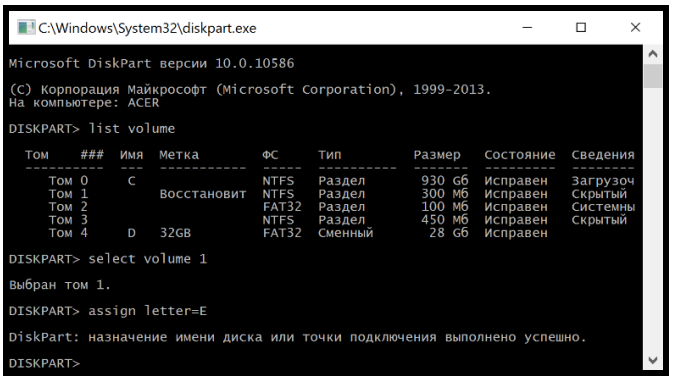

Рис. 3.1.43. Присвоение команды

Если присвоение выполнено успешно, то, не закрывая окно diskpart, перейдите в проводник и исследуйте раздел, который мы смонтировали (рис. 3.1.44).

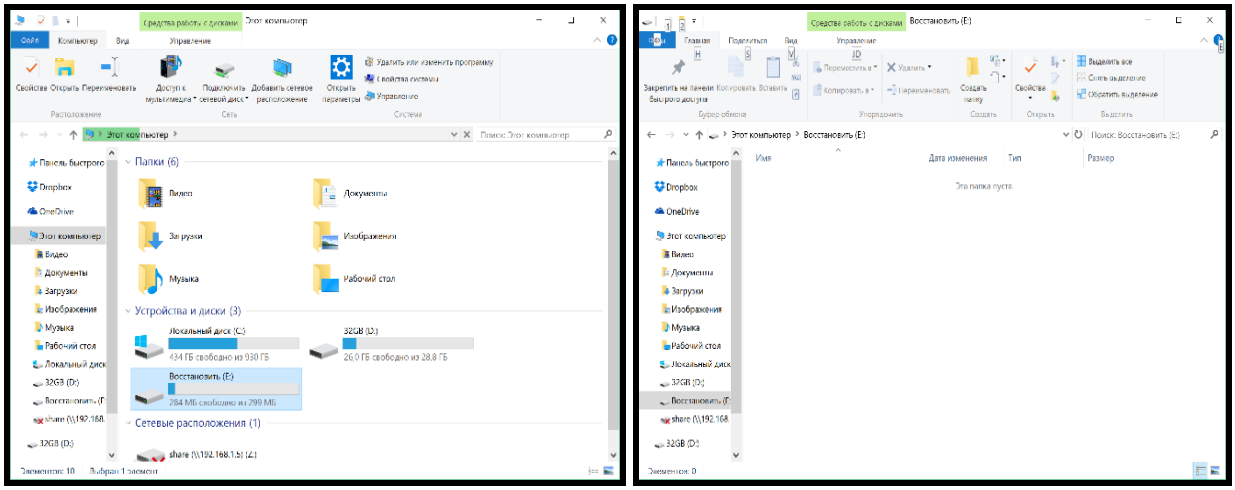

Рис. 3.1.44. Смонтированный раздел

Выполним размонтирование раздела. Это выполняется командой: remove letter=<буква>. В данном случае команда будет выглядеть remove letter=E (рис. 3.1.45).

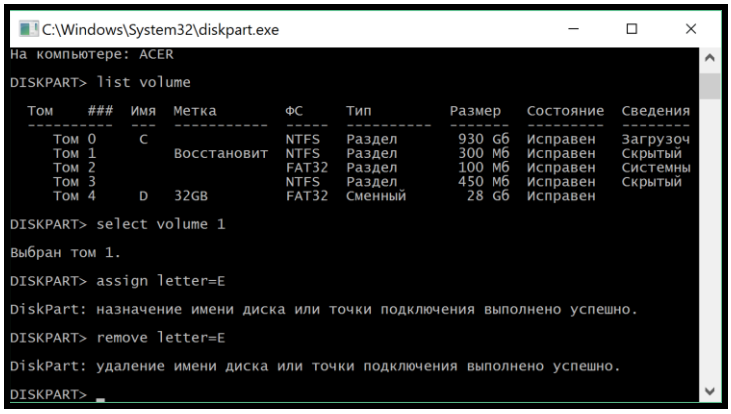

Рис. 3.1.45. Размонтирование тома

Самостоятельно выполните монтирование остальных скрытых и системных разделов и опишите, что там находится. По окончании, размонтируйте скрытые разделы.

Поиск файлов в ОС Windows

В данном учебном задании требуется найти на диске файлы и папки, имя которых содержит слово «договор». Для поиска применяются стандартные поисковые средства операционной системы Windows.

Для выполнения учебного задания выполните следующие действия:

1. Осуществите старт программы поиска.

2. Нажмите кнопку «Пуск», расположенную в нижнем левом углу рабочего стола. В поисковой строке введите слово «договор» (рис. 3.1.46).

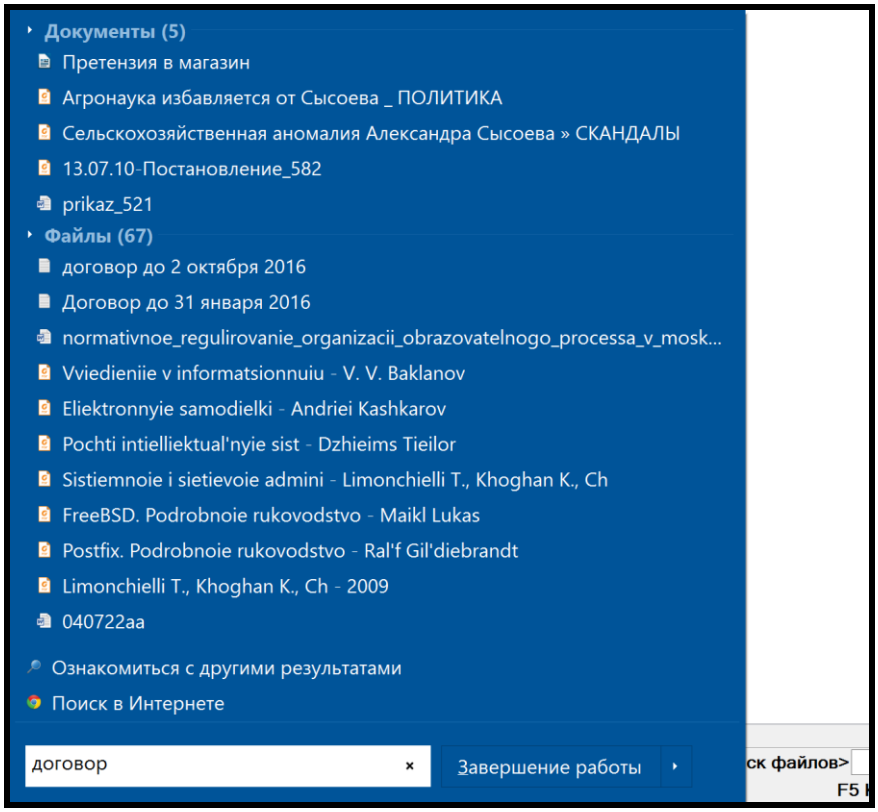

Рис. 3.1.46. Меню «Пуск»

Либо откройте окно проводника и в правом верхнем углу, введите в поисковую строку нужную фразу.

Задайте имя файла и область поиска. В поле «Имя» введите с клавиатуры слово «договор». Для переключения раскладки клавиатуры с русского языка на английский и наоборот нажмите клавиши «Ctrl+Shift». На панели инструментов выберете «Этот компьютер» (рис. 3.1.47).

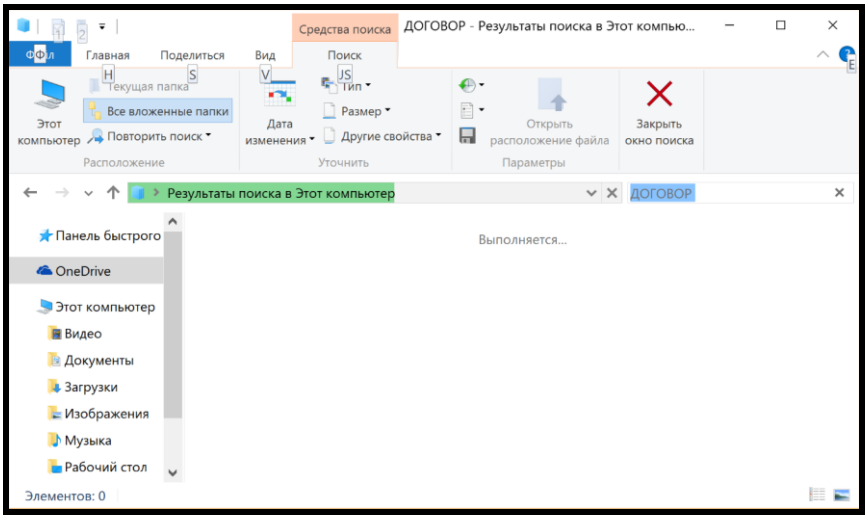

Рис. 3.1.47. Окно поиска

Осуществите поиск файлов. Нажмите на кнопку Enter. По окончании поиска в нижней части экрана появится поле со списком найденных файлов и папок (рис. 3.1.48).

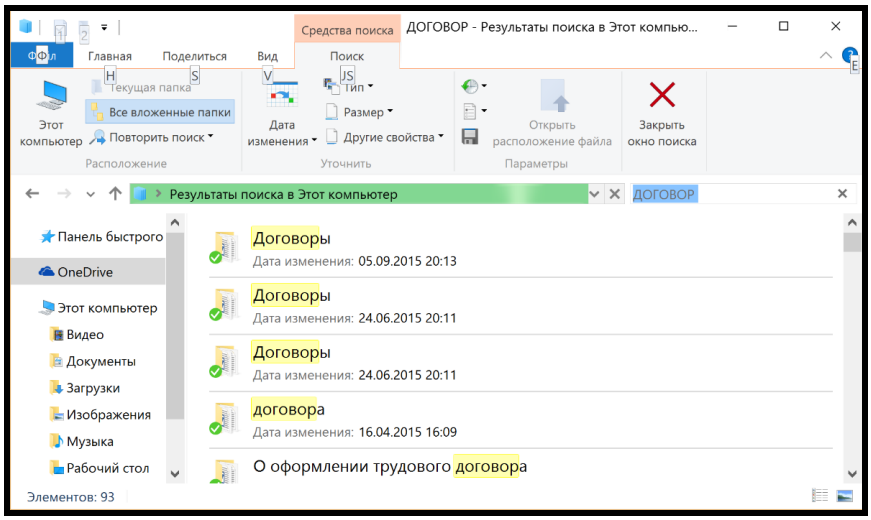

Рис. 3.1.48. Результаты поиска

Поиск файлов средствами Windows по дате создания

В данном учебном задании требуется найти файлы на диске созданные в период с 1 по 7 января 1999 г. Для выполнения учебного задания выполните следующие действия: Задайте условия поиска и введите диапазон дат. Впишите в поисковое поле «датасоздания:» и нажмите Enter. Введите необходимые промежутки времени (рис. 3.1.49).

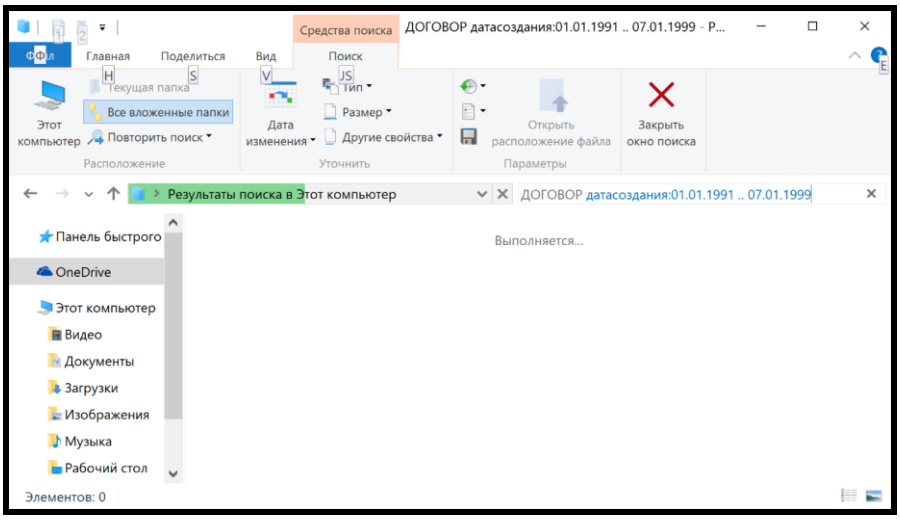

Рис. 3.1.49. Ввод параметров поиска

Осуществите поиск файлов. Поиск файлов по типу

В данном учебном задании требуется найти на диске все документы Microsoft Word.

Для выполнения учебного задания выполните следующие действия:

– восстановите стандартные условия поиска;
– введите тип файла;
– осуществите поиск файлов.

В поисковую строку введите выражение «*.doc?» (рис. 3.1.50).

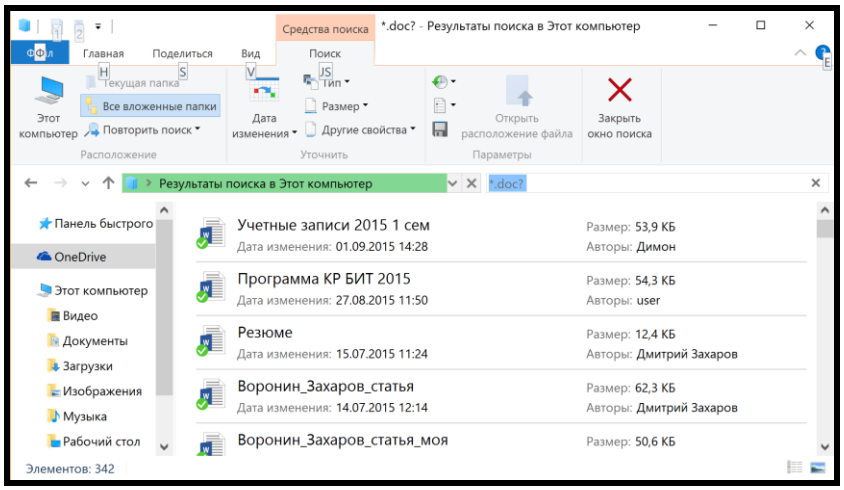

Рис. 3.1.50. Ввод параметров поиска

Поиск файлов по размеру

В данном учебном задании требуется найти на диске все документы Microsoft Word размером не менее 25 КБайт.

Для выполнения учебного задания выполните следующие действия:

– введите размер файла;
– в поисковую строку введите «размер:<25Кб»;
– осуществите поиск файлов (рис. 3.1.51).

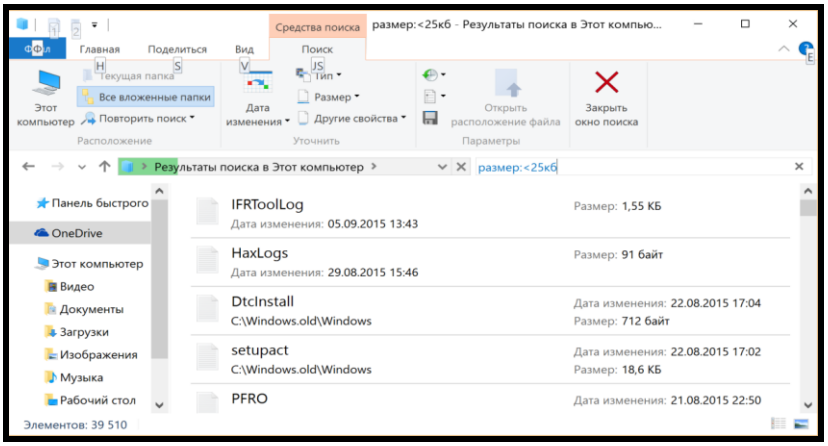

Рис. 3.1.51. Ввод параметров поиска

Поиск файлов по контексту

В данном учебном задании требуется найти файлы, содержащие слово «иванов». Поиск файлов по всему диску может занять довольно длительное время, поэтому необходимо область поиска ограничить папкой «C:\Razvedka»

Для выполнения учебного задания выполните следующие действия:

– задайте область поиска;

– перейдите в папку «C:\Razvedka». Нажмите на панели инструментов кнопку «Текущая папка». Нажмите кнопку «Дополнительные параметры» и выберете содержимое файлов (рис. 3.1.52).

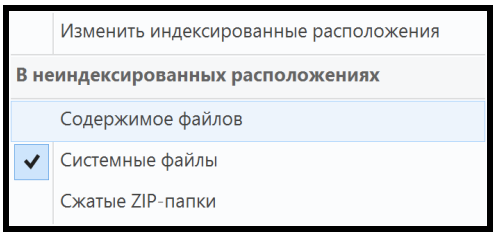

Рис. 3.1.52. Дополнительные параметры поиска

Введите текст для поиска. В поле поиска введите «иванов» (рис. 3.1.53).

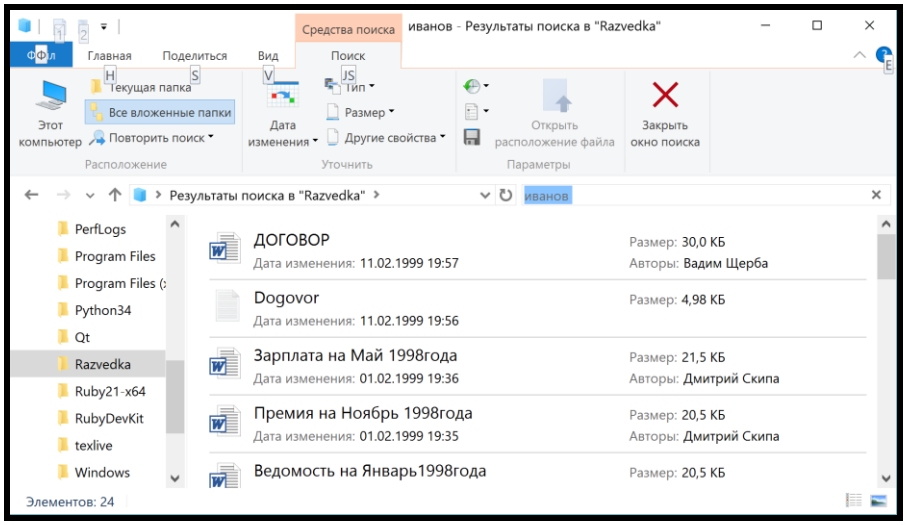

Рис. 3.1.53. Поиск файлов

Осуществите поиск файлов. Поиск среди скрытых файлов

Настройки операционной системы позволяют «прятать» от пользователя файлы с установленными атрибутами «скрытый» или «системный». Эти настройки распространяются и на поисковые средства операционной системы. Поэтому для поиска файлов с установленными атрибутами «скрытый» или «системный» предварительно необходимо осуществить настройку необходимых параметров.

В данном учебном задании требуется найти на диске текстовые файлы (с расширением «.txt»), содержащие слово «иванов» среди файлов с установленным атрибутом «скрытый файл». Для выполнения учебного задания выполните следующие действия: Установите поиск в системных файлах (рис. 3.1.54).

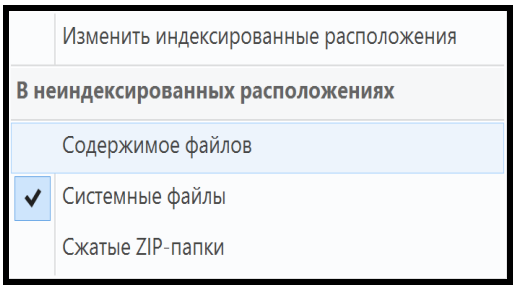

Рис. 3.1.54. Поиск в системных файлах

Осуществите поиск файлов. Поиск выполняется так же, как в предыдущем учебном задании. В окне результатов поиска скрытые файлы отображаются бледными значками.

Поиск файлов средствами Total Comander по имени

В данном учебном задании требуется найти в папке «C:\Razvedka\» все файлы, с именем «Договор.doc».

Для выполнения учебного задания выполните следующие действия:

– осуществите старт программы «Total Comander»;
– пуск – Все программы – Total Comander;
– включите режим поиска;
– нажмите клавиши «Alt – F7», появится окно поиска (рис. 3.1.55).

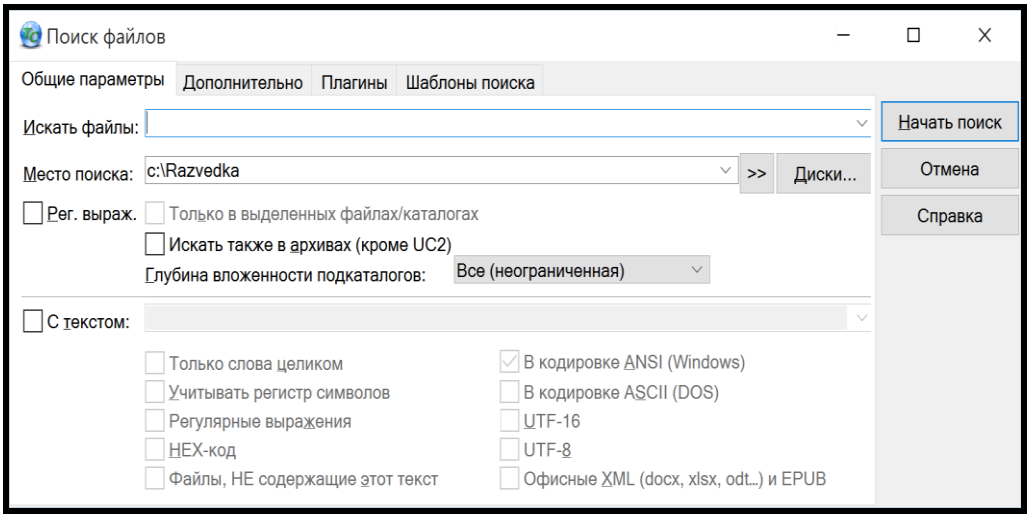

Рис. 3.1.55. Режим поиска

Введите имя файла и условия поиска. В поле «Искать файлы» введите с клавиатуры «ДОГОВОР.doc». Осуществите поиск файлов. Нажмите на кнопку «Начать поиск». В нижней части окна будут отображаться найденные файлы (рис. 3.1.56).

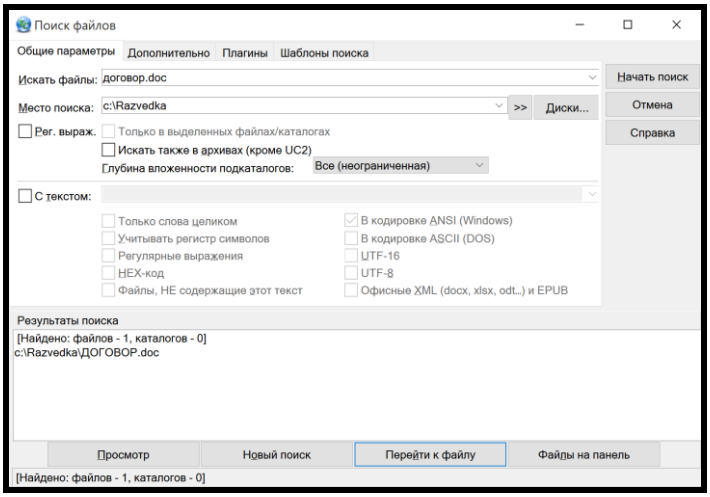

Рис. 3.1.56. Результаты поиска

Поиск файлов средствами Total Comander по фрагменту имени

Если неизвестен тип файла, или известна только часть имени, то вместо имени можно указывать шаблон. В шаблоне помимо обычных букв можно использовать специальные символы:

? – заменяет один любой символ;

* – заменяет любую группу символов.

Так, по шаблону «???.*» будут обнаружены файлы, имя которых состоит из трех букв, а по шаблону «?og*.d*» будут обнаружены файлы, в имени которых вторая и третья буквы «og» и расширение начинается на букву «d» например: «dogovor.doc», «pogoda.dat», «dog.dr».

В данном учебном задании требуется найти в папке «C:\Razvedka\» все файлы, имя которых начинается с «dog». Для выполнения учебного задания выполните следующие действия: введите условия поиска. В поле «Искать файлы» введите с клавиатуры «dog*.*» (рис. 3.1.57).

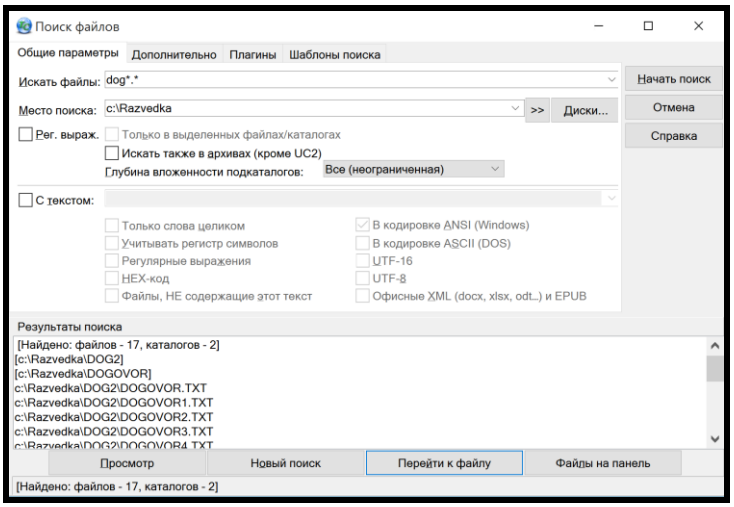

Рис. 3.1.57. Результаты поиска

Осуществите поиск файлов. Самостоятельно осуществите поиск файлов, имя которых заканчивается на «4».

Поиск файлов средствами Total Comander по типу файла

В данном учебном задании требуется найти в папке «C:\Razvedka\» все файлы, созданные при помощи текстового редактора Microsoft Word. Документы Microsoft Word, как правило, имеют расширение «.doc» и «.docx».

Для выполнения учебного задания выполните следующие действия:

– введите условия поиска;

– в поле «Искать файлы» введите с клавиатуры «*.doc»;

осуществите поиск файлов.

Поиск файлов средствами Total Comander по контексту

В данном учебном задании требуется найти в папке «C:\Razvedka\» документы, в которых речь идет о продаже. Программа, осуществляющая поиск не способна учитывать правила грамматики русского языка, поэтому в качестве строки для контекстного поиска целесообразно взять слово без окончания, в данном примере – «продаж». Для выполнения учебного задания выполните следующие действия: Введите условия поиска. Установите переключатель «С текстом» и введите слово «продаж» (рис. 3.1.58). Осуществите поиск файлов.

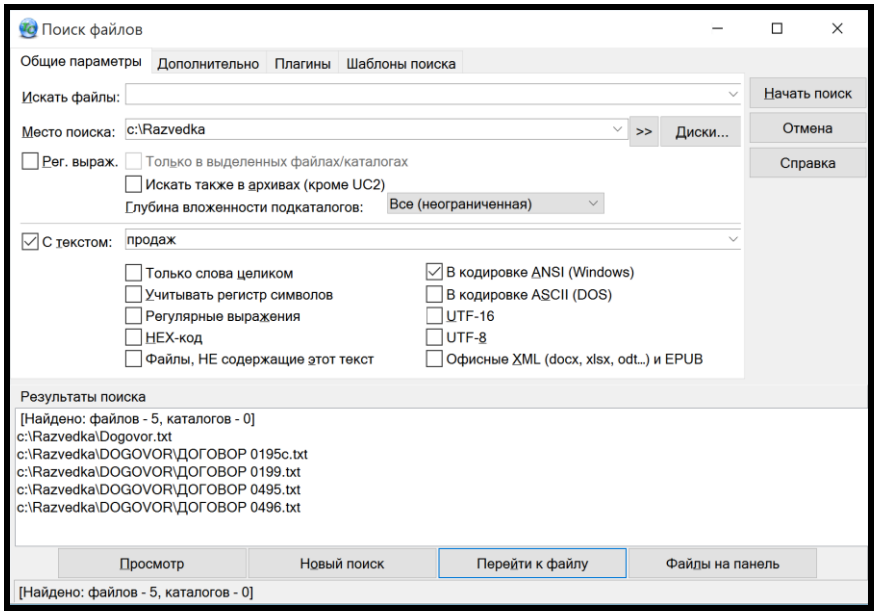

Рис. 3.1.58. Поиск файлов

Просмотр и поиск внутри файла средствами Total Comander

Программа «Total Comander» имеет встроенные средства для просмотра текстовых файлов, которые позволяют просматривать файлы нескольких различных форматов, использующих кодировки CP866 (стандартная кодировка DOS) и CP1251 (стандартная кодировка Windows).

В данном учебном задании требуется осуществить просмотр текстовых файлов, использующих различную кодировку, а также поиск строки «Иванов» внутри файла. Для выполнения учебного задания выполните следующие действия: Перейдите к папке «C:\Razvedka\».

В указанной папке расположены три документа, использующие различные кодировки:

– договор.txt – кодировка CP866;
– dogovor.txt – кодировка CP1251;
– договор.doc – кодировка UNICODE.

Осуществите просмотр документов с различными кодировками, затем для переключения в режим просмотра выберите файл и нажмите клавишу «F3». Откроется окно просмотра документа.

Если в файле используется кодировка CP866 (стандартная кодировка DOS), то в окне будет отображен текст. Если же в файле используется иная кодировка, то в окне будет отображен нечитаемый набор символов. В таком случае необходимо переключить программу просмотра в кодировку CP1251 (стандартная кодировка Windows). Для этого в меню «Кодировка» последовательно выбирайте кодировку, пока текст не станет читаемым. Если текст по-прежнему прочитать невозможно, значит в файле используется кодировка UNICODE, и просмотреть его средствами Total Comander невозможно.

Для выхода из режима просмотра документа нажмите клавишу «ESC». Осуществите поиск строки внутри текстового файла. Для поиска строки внутри текстового файла нажмите в режиме просмотра клавишу «F7». В появившемся окне в поле введите искомую строку «Иванов» и нажмите клавишу «Enter».

В случае успешного поиска обнаруженная строка выделяется в тексте. Для продолжения поиска нажмите «Shift+F7». По достижении конца документы будет выведено соответствующее сообщение (рис. 3.1.59).

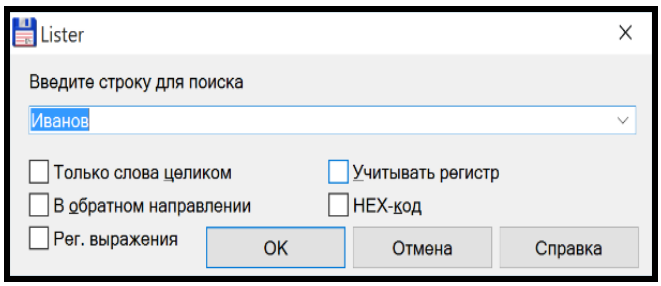

Рис. 3.1.59. Строка для поиска

Применение специализированного программного обеспечения для поиска информации. Помимо поисковых средств, встроенных в операционную систему, и прикладных программ существует и специализированное программное обеспечение, предназначенное исключительно для поиска информации на диске и обладающее более широкими возможностями для поиска.

Изучение возможностей поиска информации при помощи программы AVSearch

Выполните самостоятельное изучение возможностей программы AVSearch. Данная программа предназначена для поиска файлов на дисках по фрагментам текста в любой кодировке: Windows1251, OEM 866 (DOS), KOI-8R, ISO 8859-5, UNICODE. Имеется возможность поиска в различных архивах (около 20 форматов). Встроенные средства позволяют просматривать найденные документы в текстовом или шестнадцатеричном виде, осуществлять поиск внутри файлов, сохранять список файлов для дальнейшей об-

работки, производить различные файловые операции (удаление, переименование, копирование), задавать в качестве области поиска набор папок и многое другое.

Просмотр файлов эскизов изображений thumbs.db

С помощью любой поисковой программы найдите файлы thumbs.db, например с помощью Total Comander (рис. 3.1.60, 3.1.61, 3.1.62).

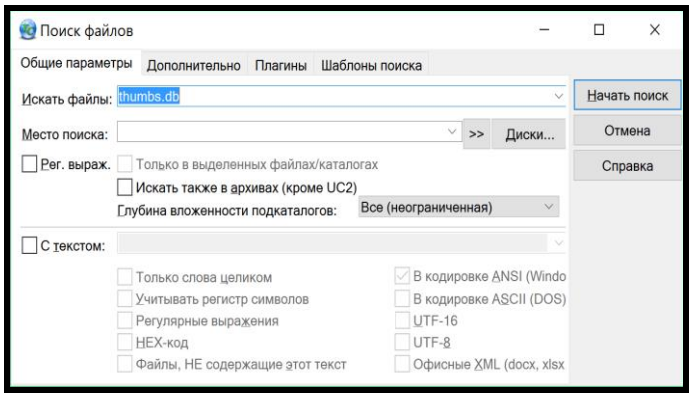

Рис. 3.1.60. Поиск файлов в Total Comander

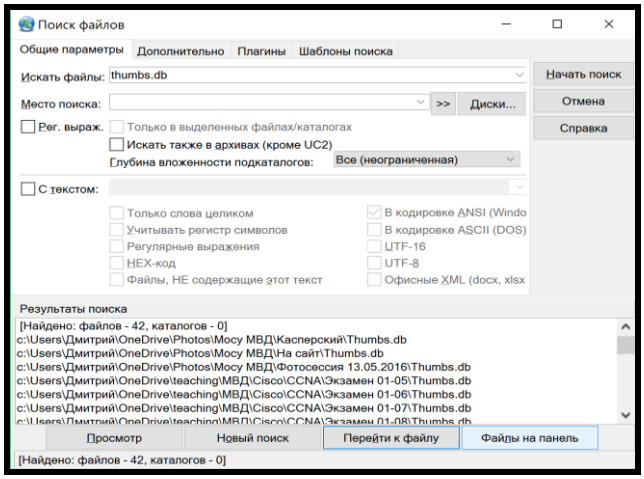

Рис. 3.1.61. Поиск файлов в Total Comander

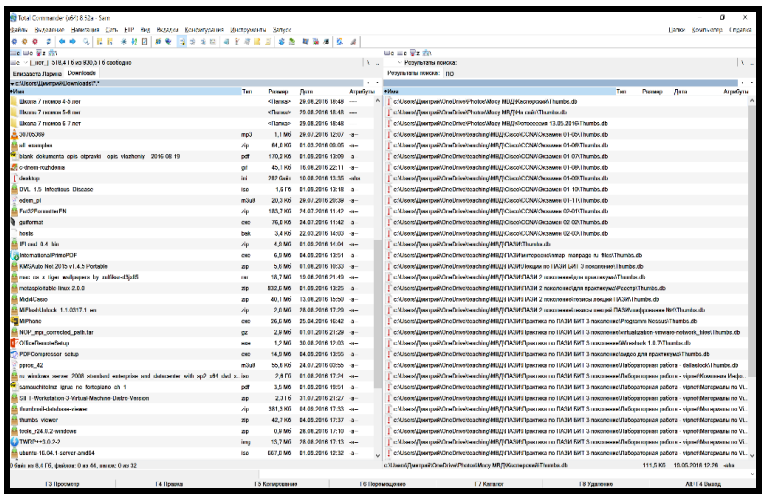

Рис. 3.1.62. Поиск файлов в Total Comander

Нажмите начать поиск, затем кнопку Файлы на панель.

Выполните просмотр с помощью утилиты thumbs viewer. Для этого запустите ее и перетащите любой из найденных файлов в нее (рис. 3.1.63).

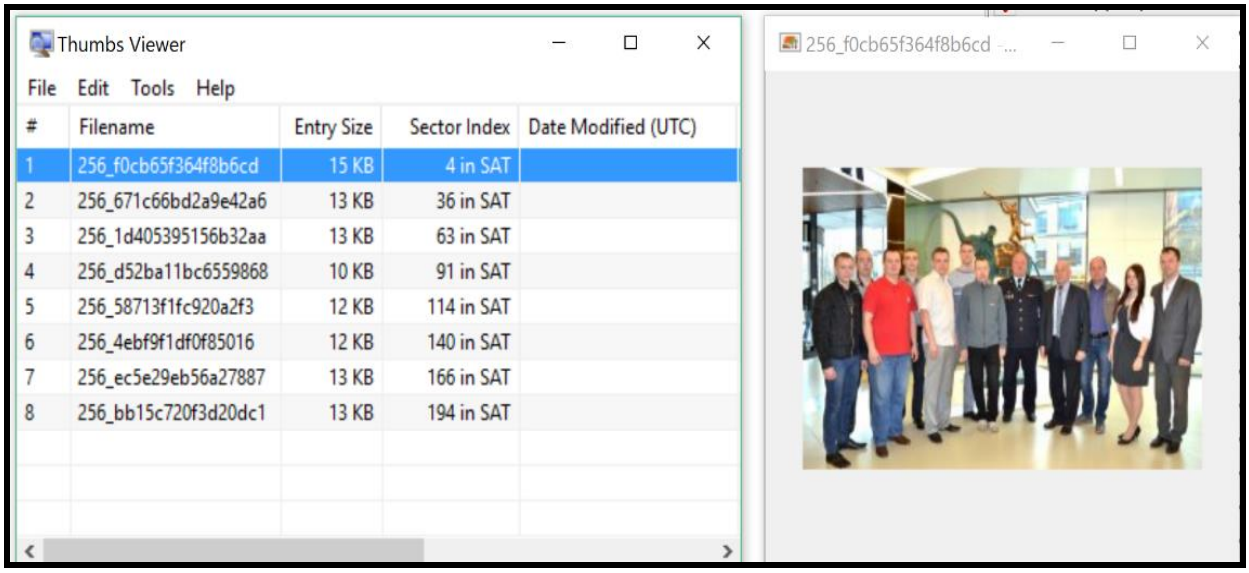

Рис. 3.1.63. Thumbs viewer

§ 3.2. Восстановление и поиск компьютерной информации

Осмотр объектов, поступивших на экспертизу

Осмотр объектов, поступивших на экспертизу, начинается с проведения экспертного исследования составляющих персонального компьютера на предмет их функционального назначения, исправности, возможности совместного использования компьютера и периферийного оборудования.

Компьютерно-техническая экспертиза (КТЭ) может проводиться при производстве расследования по уголовным и гражданским делам, делам об административных правонарушениях, в арбитражных спорах, при проведении внутренних расследований и в иных случаях.

Исследование компьютерной техники необходимо для всестороннего изучения средств и систем, обрабатывающих либо хранящих электронную информацию, с целью получения доказательственных, разыскных и ориентирующих данных.

Таким образом, в рамках проведения компьютерно-технической экспертизы могут быть исследованы такие устройства, как:

– персональные компьютеры;

– ноутбуки;

– планшеты;

– мобильные устройства (телефоны, смартфоны и т. п.);

– устройства хранения данных («флешки», внешние жесткие диски, оптические диски и т. д.);

– иные устройства, содержащие компьютерную информацию.

Этапы получения упакованных объектов экспертизы

1. Сверка представленных объектов экспертизы с указанными в постановлении.
2. Контроль целостности упаковки объектов.
3. Фотосъемка упаковки объектов.
4. Занесение в постановление записи о получении постановления и объектов экспертизы. При необходимости указать, что объекты в запечатанной упаковке, которая при получении не вскрывалась. Указать иные замечания. «Постановление и объекты экспертизы, упакованные в запечатанную картонную коробку белого цвета, получил. При получении вскрытие упаковки не производилось».
5. Подпись в постановлении.

Описание упаковки объектов

Отличительные особенности упаковки объектов, на которые стоит обратить внимание при описании:

1. Свойства упаковки: тип (конверт, коробка, сложенный лист бумаги, кипкейс), материал (бумажный, картонный, полимерный), цвет (черный, белый, лазурный).
2. Надписи на поверхности упаковки с указанием цвета. При этом на упаковке могут быть надписи, маркировочные обозначения, так и рукописные надписи, которые следует интерпретировать без домысливания и указывать «читаемые как : ». Не следует исправлять орфографию, трактовая переносы (новая строка – новая надпись).
3. Оттиски печати (без домысливания не пропечатанных надписей) с указанием формы, цвета. Подписи с указанием цвета, расшифровкой или без нее.
4. Листы бумаги или прочие объекты, которые приклеены к упаковке, и на которых также могут присутствовать надписи, оттиски, подписи.
5. Оклейка упаковки объекта клейкой лентой прозрачной или цветной.
6. Суждение о целостности упаковки[1].

Поверхность коробки оклеена прозрачной клейкой лентой. Также с помощью этой клейкой ленты к поверхности коробки приклеен лист бумаги белого цвета, на поверхности которого присутствуют надписи черного цвета следующего содержания:

С помощью визуального осмотра установлено, что целостность данной картонной коробки не нарушена. Фотоснимки упаковки объектов, полученных на экспертизу.

Фотосъемка объектов экспертизы

Рекомендации при фотосъемке упаковки справедливы и для объектов экспертизы. Последовательность фотосъемки составных объектов, представлены на рис. 3.2.1:

---

[1] Представленные на экспертизу объекты упакованы в картонную коробку, на поверхности которой могут присутствовать различные надписи, например, «ЛАЗЕРНЫЙ», «ПРИНТЕР», «КОПИРОВАЛЬНЫЙ», «АППАРАТ», «ФАКСОВЫЙ», «АППАРАТ», «ОБРАЗЕЦ», «КАЧЕСТВА», «А4», «210 х 297 мм», «ТОВАР ГОДА 2019 и 2020», а также надписи, читаемые как «2 г», «0808|204». На поверхность коробки приклеены четыре листа бумаги белого цвета, на поверхности каждого из которых присутствует оттиск круглой печати синего цвета: «УПРАВЛЕНИЕ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО … ОБЛАТИ», «МВД РФ», «Печать», «для пакетов», «№…».

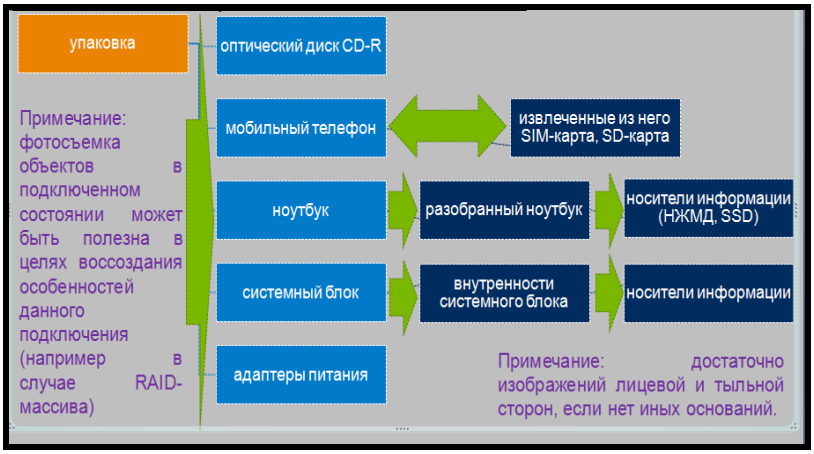

Рис. 3.2.1. Последовательность фотосъемки

Фиксирование выявленных физических повреждений объекта экспертизы

Наиболее частый случай – треснутый экран мобильного телефона (рис. 3.2.2).

Рис. 3.2.2. Разбитый телефон

С помощью визуального осмотра были обнаружены признаки множественных внешних повреждений устройства, а именно треснутый экран, поврежденный, не закрывающийся корпус.

Тип оптического носителя данных, оценка его состояния

Оценка состояния оптического носителя данных:

1. Наличие царапин, их глубина (повреждение лакового защитного слоя), местоположение (в пустой или в области записанных данных).

2. Загрязнение поверхности. Чистка данной поверхности ватной палочкой и нейтральными жидкостями (водой), растворителями (при отсутствии реакции на него покрытия диска).

При этом, любые действия, которые могут привести к необратимым последствиям, должны выполняться только после зафиксированного согласия следователя, с информированием его о рисках.

Форматы оптических носителей информации (рис. 3.3.3):

– CD (оптический носитель информации в виде пластикового диска с отверстием в центре, процесс записи и считывания информации которого осуществляется при помощи лазера);

– DVD (носитель информации, выполненный в форме диска, имеющего такой же размер, как и компакт-диск, но более плотную структуру рабочей поверхности, что позволяет хранить и считывать больший объем информации за счет использования лазера с меньшей длиной волны и линзы с большей числовой апертурой[1]);

– BD (формат оптического носителя, используемый для записи с повышенной плотностью хранения цифровых данных, включая видео высокой четкости).

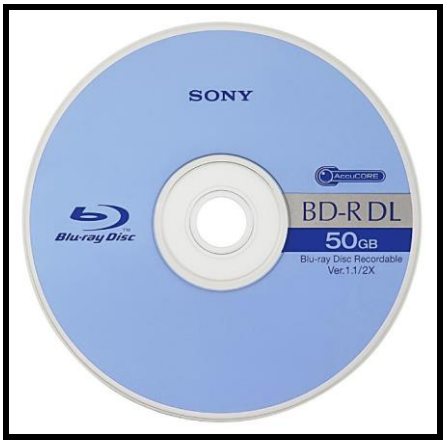

Рис. 3.3.3. Оптический носитель информации

Предотвращение записи при исследовании оптических носителей данных.

При исследовании оптических носителей данных явной необходимости в применении программных или аппаратных блокираторов записи не наблюдается.

Тем не менее все же рекомендуется использовать ОС с контролируемым монтированием разделов и их автозапуском. Для этих целей, например, подойдет ОС Deft Linux, в которой отсутствует автомонтирование несистемных разделов.

Также к плюсам Unix-систем стоит отнести возможность работы с устройствами как с файлами.

Оценка сложности разбора ноутбука. Использование «live» ОС при исследовании

Факторы указывающие в пользу использования «live» ОС при исследовании ноутбука:

– наличие интегрированной памяти;

– сложность разбора, наличие клеевых соединений;

– отсутствие переходников под специфические интерфейсы;

– отсутствие специальных инструментов;

[1] Апертура (от лат. aperture – отверстие) в оптике – характеристика оптического прибора, описывающая его способность собирать свет и противостоять дифракционному размытию деталей изображения. В зависимости от типа оптической системы данная характеристика обладает линейным или угловым размером. Числовая апертура (NA) – это величина, используемая для выражения яркости или разрешающей способности оптической системы объектива; представляет собой синус угла приема, т. е.: NA=sin (01).

– наличие зарядного устройства (в случае отсутствия не рекомендуется использование «live» ОС).

При использовании «live» ОС среди основных рисков отмечают пропуск момента доступа к BIOS/UEFI (так как доступ может быть ограничен). Для ноутбуков с SSD с целью минимизации рисков важно обратить внимание на меню выбора приоритетного носителя информации (рис. 3.3.4).

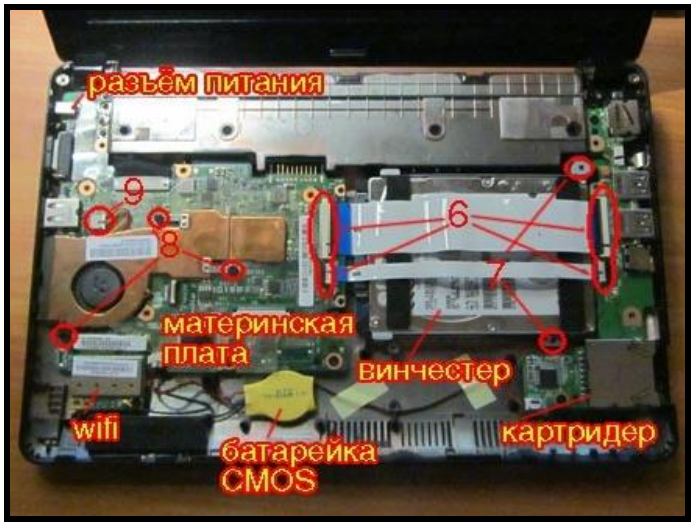

Рис. 3.3.4. Ноутбук в разобранном виде

Носители данных системного блока

К наиболее часто встречающимся в системном блоке (ПЭВМ) носителям информации можно отнести следующие:

– НЖМД (HDD);
– SSD-SATA;
– SSD-M.2;
– SSD-PCIe;
– CD;
– интегрированная память;
– аппаратный RAID-контроллер.

Исследование мобильного телефона. Подключение к стендовой ПЭВМ. Физическое извлечение данных из мобильных устройств

Так как следователей интересуют, в том числе, и удаленные данные, находящиеся в памяти мобильных устройств, судебному эксперту необходимо сделать физическое извлечение данных из памяти мобильного устройства, т. е. получить полную копию памяти исследуемого им устройства. Он может сделать физический дамп памяти мобильного устройства следующими методами:

– извлечение данных из микросхем памяти мобильного устройства методом «chip-off». Это самый трудный метод извлечения данных. Но иногда просто нет другого способа скопировать данные из устройства;

– извлечение данных из памяти мобильного устройства с использованием отладочного интерфейса JTAG. Достаточно популярный метод извлечения данных с помощью программаторов RIFF-box, Octopus и т. п. Позволяет извлекать данные из устройств, имеющих незначительные аппаратные или программные повреждения. Важно понимать, что некоторые программаторы создают дамп памяти мобильного устройства в собственном формате (отличном от RAW). Подобные дампы необходимо конвертировать в формат, который поддерживают судебные программы, имеющиеся в распоряжении судебного эксперта;

– извлечение данных с помощью специализированных программ (например, Oxygen Forensic Suit) и программно-аппаратных комплексов (XRY «Micro Systemation»), UFED (Cellebrite Forensics), Secure View 3). Подобные инструменты используют наиболее безопасный метод root-доступа к мобильным устройствам. Это означает, что судебный эксперт не всегда может получить root-доступ к устройству, однако, оно будет исправно после проведения исследования. Можно попытаться получить root-доступ иными, часто, более эффективными, способами. Однако, при этом существует вероятность повредить исследуемое мобильное устройство;

– создание копии памяти мобильного устройства в ручном режиме;

– комбинированные методы.

Например, в случае, если данные пользователя сохраняются в расширенной памяти центрального процессора мобильного устройства (такая особенность характерна для «китайских телефонов» («Chinese mobile devices», «Chinese phones»), в которых используются ARM процессоры фирм Mediatek, Spreadtrum и Infineon, возможно применение комбинации методов: извлечение данных из микросхемы мобильного устройства «chip-off» (когда из устройства выпаивается центральный процессор, в котором, в том числе, содержатся данные пользователя) и, в дальнейшем, извлечение пользовательских данных по интерфейсу JTAG.

Логическое извлечение данных. Получение доступа к данным, содержащимся в дампе памяти мобильного устройства

Каким бы способом судебный эксперт не получил дамп памяти мобильного устройства, в конечном счете он получит файл (или несколько файлов) которые надо как-то исследовать и извлечь из него нужные данные.

Если задачей судебного эксперта является извлечение только логических данных, содержащимся в дампе мобильного устройства, он может смонтировать полученный образ FTK Imager или UFSExplorer. Дампы памяти мобильных устройств, как правило, содержат большое количество логических разделов.

Если судебный эксперт исследует файл, представляющий собой копию логического раздела мобильного устройства, имеющий файловую систему YAFFS2, он может получить доступ к логическим данным, содержащимся в нем, с использованием Encase Forensic версии 7.

Декодирование SQLite баз данных

Как правило, SQLite базы данных, извлеченные из дампа памяти мобильного устройства, неизменно представляют большой интерес для судебного эксперта. Прежде всего это связано с тем, что большое количество криминалистически значи-

мых данных мобильные устройства хранят именно в этом формате. В SQLite базах данных хранятся следующие данные мобильного устройства: телефонная книга, вызовы, СМС-сообщения, MMS-сообщения, словари, данные веб-браузеров мобильного устройства, системные журналы мобильного устройства и т. д.

Восстановление удаленных данных и файлов

Восстановление данных и файлов из мобильных устройств – это сложный процесс. Связано это с аппаратной организацией хранения данных в микросхемах памяти мобильных устройств и с особенностями файловых систем мобильных устройств. Это необычно, но, большинство судебных программ не поддерживает файловую систему YAFFS2. Поэтому при исследовании физических дампов мобильных устройств, судебный эксперт может оказаться в ситуации, когда его любимая программа восстановления данных окажется неспособна восстановить хоть что-нибудь из дампа памяти подобного мобильного устройства. Как показывает наша практика, из подобных дампов достаточно сложно восстановить удаленные видеофайлы и иные файлы больших размеров. Определенную сложность может вызывать восстановление удаленных данных из дампов памяти мобильных устройств, содержащих файловые системы YAFFS2.

Приоритетность идентификации мобильного телефона с точки зрения методов исследования:

- точная модель мобильного телефона;
- модель телефона с идентичным процессором;
- модель телефона с близким в семействе процессором;
- универсальный метод для телефонов конкретного семейства;
- телефон с идентичной версией ОС.

При исследовании необходимо обеспечить условия, препятствующие возможной передаче данных устройством.

Для некоторых моделей телефонов возможно извлечением их содержимого без необходимости запуск ОС Android (семейство MTK). Решается проблема неисправного экрана. Данные могут быть зашифрованы.

Рис. 3.3.5. UFED

В настройки ОС мобильного телефона были внесены следующие изменения: в подразделе «Разработка» раздела «Приложения» были установлены галочки напротив пунктов «Отладка USB», «Оставить включенным». Описанные выше изменения необходимы для проведения анализа содержимого мобильного устройства с помощью ПО «UFED 4PC», «UFED Physical Analyzer» (рис. 3.3.5). Исследуемый мобильный телефон «SONY XPERIA» был безопасно отключен от стендовой ПЭВМ, настройки ОС приведены к изначальному состоянию, в последующем мобильный телефон был выключен.

Chip-off как метод извлечения информации

Метод заключается в том, что из поврежденного мобильного устройства извлекается чип памяти и устанавливается в точно такое же исправное мобильное устройство. При этом решается сразу несколько сложных задач, с которыми пришлось бы столкнуться, используя метод chip-off.

Перепайка чипа – это очень сложная и трудоемкая работа. Существует вероятность стирания данных из-за воздействия высоких температур на чип или его механическое повреждение (рис. 3.3.6).

Также нельзя исключать, что производитель мобильного устройства использует аппаратную защиту, которая при замене чипа памяти в устройстве сотрет все данные.

Перед тем как проводить исследование поврежденного мобильного устройства, целесообразно использовать аналогичное устройство, для этого необходимо поменять их чипы памяти местами и посмотреть на реакцию устройств. При использовании данного метода необходимо оборудование для реболлинга (инфракрасная паяльная станция) – это процесс восстановления шариковых выводов электронных BGA-компонентов. BGA – это разновидность корпуса интегральных микросхем, поверхностно монтируемых на электронной плате. BGA-выводы представляют собой шарики из припоя, нанесенные на контактные площадки с обратной стороны микросхемы.

Применимо к flash-памяти на SSD-, USB-, SD-носителях информации, мобильных телефонах (данные могут быть зашифрованы), которые можно собрать из нескольких микросхем памяти и выбрать тип контроллера.

Данные действия могут привести к необратимым последствиям.

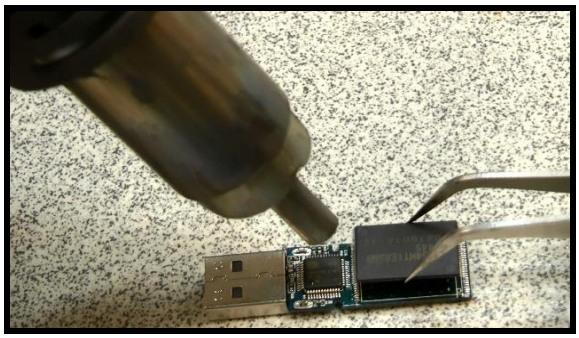

Рис. 3.3.6. Перепайка чипа

Плюсы данного метода заключаются в возможности восстановления данных при сильном повреждении мобильного устройства. Стоит отметить, что у данного метода есть и минусы:

– для извлечения чипа требуется полная разборка устройства, что занимает много времени, и зачастую может привести к потере работоспособности устройства;

– требуется дорогостоящее оборудование и достаточно дорогое ПО;

– отечественная практика при проведении КТЭ показывает, что должностные лица, осуществляющие следствие в рамках уголовного дела или проверки, скептически относятся к методу chip-off и редко идут на разрешение подобных мер.

Внешние проявления повреждений электронных компонент печатных плат (объекта экспертизы)

Рис. 3.3.7. Вздувшиеся конденсаторы

Рис. 3.3.8. Гарь на плате

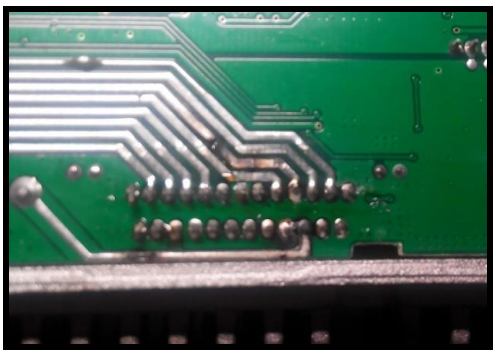

Рис. 3.3.9. Выгорание, обрыв токопроводящих дорожек

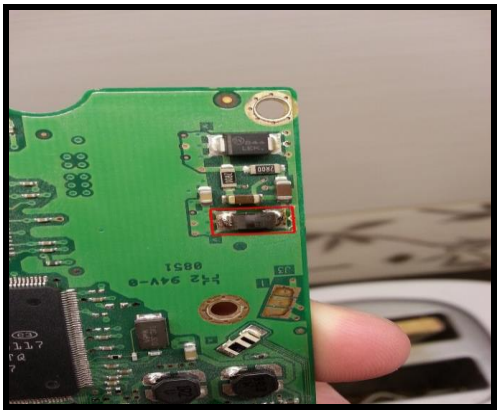

Рис. 3.3.10. Выгорание SMD-компонент (резисторов, диодов)

Рис. 3.3.11. Повреждение контроллера

Иные способы выявления повреждений объекта экспертизы

1. Звук, не свойственный корректной работе устройства.
2. Запах горелого.
3. Диагностика специальными средствами.

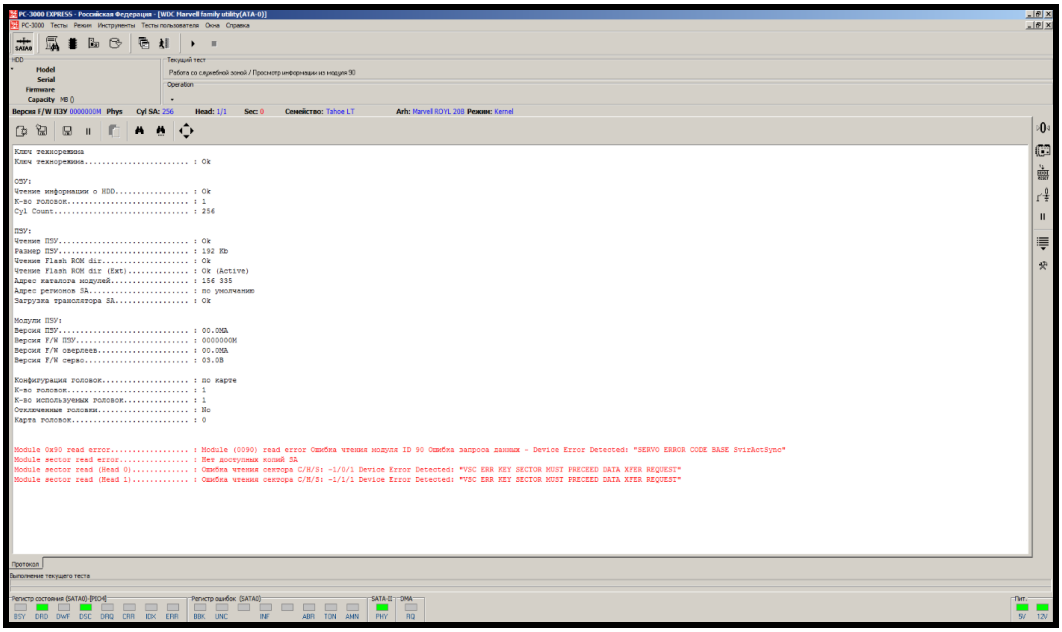

Рис. 3.3.12. Пример для НЖМД – аппаратно-программный комплекс PC-3000

Интерфейсы подключения носителей данных

Характеристики интерфейсов подключения:

– размер контактной группы;
– количество пинов;
– размер пинов;
– расположение ключа;
– размер платы;
– назначение пинов.

Предотвращение записи при исследовании HDD, SSD

При исследовании HDD, SSD обязательным условием является применение аппаратных и/или программных блокираторов записи.

Реализации аппаратных блокираторов:

– в качестве модулей, предоставляющих доступ к блочному устройству;
– в качестве транслятора команд;
– ОС с контролируемым монтированием разделов и их автозапуском. К таким ОС можно отнести ОС Deft Linux, в которой отсутствует автомонтирование не системных разделов;
– программы (драйвера), осуществляющие перехват запросов на запись данных, блокируя их или перенаправляя в кэш.

Плюсы:

– больший контроль (уверенность) предотвращения записи;
– независимость от ОС хоста. (программная блокировка может быть преодолена с помощью ВПО);
– моментальное предотвращение записи, нет необходимости дожидаться инициализации ОС, исключено воздействие загрузчика хоста, сервисов EFI, прерывания BIOS 0x13;
– комфортные условия для работы объекта исследования. (стабилизированное точное напряжение, запас по нагрузочной способности).

Минусы:

– необходимость обладания устройством;
– меньшая скорость чтения данных.

Работа с сетевыми системами хранения данных (NAS)

Иногда единственный вариант – запуск NAS с клонами его носителей информации. Всегда стоит фиксировать порядок подключения носителей информации NAS.

Носители информации сетевых систем хранения данных (NAS) чаще всего подключены по схеме RAID-массивов. При этом возможно использование нестандартных схем, так для NAS Synology – Synology Hybrid RAID, реконструкция которого может представлять сложности.

Реконструкцию стандартных RAID-массивов носителей возможно осуществлять с помощью ПО R-Studio, UFS Explorer, WinHEX, mdadm.

Извлечение информации накопителей данных нестандартных устройств.

Факторы, которые необходимо учитывать:

– схемотехника окружения чипа памяти;

– организация правильного питания.

Возможность физического, термического, электростатического повреждения элементов платы, включая чип памяти.

Любые действия, которые могут привести к необратимым последствиям, должны выполняться только после зафиксированного согласия следователя, с информированием его о рисках.

§ 3.3. Поиск компьютерной информации. Анализ артефактов ОС Windows для получения доказательств

Правильный и грамотный анализ компьютерных инцидентов необходим для решения поставленных перед экспертом задач. Специалист должен уметь анализировать артефакты операционной системы Windows (далее – ОС Windows) на предмет наличия в них следов компьютерных преступлений, чтобы уметь воссоздать ясную картину произошедшего, а именно какой пользователь совершал действия, какие это действия, когда он их совершал, каков механизм и т. п.

Далее описаны артефакты ОС Windows, изучение которых позволит точнее определить действия, происходившие в системе. В некоторых случаях ряд артефактов принадлежат одной области деятельности, это своеобразные маркеры, которые помогут ответить на важные вопросы расследования компьютерных инцидентов.

Загрузчики файлов

Открытие/сохранение MRU (от англ. maximum receive unit) – это максимальный размер данных, передаваемых в пакете протокола PPP, не включая заголовок пакета.

Данный ключ отслеживает файлы, которые были открыты или сохранены в диалоговом окне оболочки Windows. Это большой набор данных не только включает в себя веб-браузеры, такие как IE, Chrome и Firefox, но и большинство часто используемых приложений.

Расположение ключа:

– XP: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU;

– Win7/8/10: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU.

Описание пути к ключу:

«*» – этот параметр отслеживает самые последние файлы любых входных расширений в диалоговом Open/Save.

«.???» – это параметр предоставляет информацию о файле в диалоговом окне Open/Save конкретных расширений.

Вложения электронной почты

Большое количество файлов передается через вложения электронной почты. Стандарты электронной почты позволяют смотреть только текст. Вложения должны быть закодированы с MIME (формат base64).

Расположение электронной почты Outlook:

– XP: %USERPROFILE%\Local Settings\ApplicationData\Microsoft\Outlook;

– Win7/8/10: %USERPROFILE%\AppData\Local\Microsoft\Outlook.

Описание электронной почты Outlook:

Файлы данных MS Outlook, найденные в этих местах, включают OST и PST файлы. Также необходимо проверить их содержание. Следует учитывать конкретную версию MS Outlook для нахождения папок данного почтового клиента.

История Skype

Историю Skype сохраняет лог-файл чата сессий и файлов, передаваемых из одной машины на другую. Это включено по умолчанию в установки Skype.

Расположение истории Skype:

– XP: C:\Documents and Settings\<username>\Application\Skype\<skype-name>;

– Win7/8/10: C:\%USERPROFILE%\AppData\Roaming\Skype\<skype-name>.

Описание истории Skype:

Каждая запись будет иметь значение даты/времени и имени пользователя Skype, связанные с его действием.

Артефакты веб-браузеров

Данный раздел не относится непосредственно к операции «Скачать файл». Детали хранятся для каждой локальной учетной записи пользователя, в частности количество записей о посещениях (частота).

Расположение артефактов Internet Explorer, Firefox, Chrome

Internet Explorer:

– IE8-9: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat;

– IE10-11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat.

Firefox:

– v3 25: %userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite;

– v26+: %userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\places.sqlite Table:moz_annos.

Chrome:

– Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\UserData\Default\History.

О*писание артефактов веб браузера:*

В истории появится список файлов, которые были открыты на удаленных сайтах и загружены в локальную систему. Для получения доступа к файлу на сайте следует перейти по ссылке.

Загрузки Firefox и IE имеют встроенный диспетчер приложений, который хранит в себе историю каждого файла, загруженного пользователем. Это артефакт браузера содержит важную информацию о том, какие сайты пользователь посещал и какие файлы он скачал с них.

Расположение Firefox:

– XP: %userprofile%\Application Data\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite;

– Win7/8/10:%userprofile%\AppData\Roaming\Mozilla\ Firefox\ Profiles\<random text>.default\downloads.sqlite.

Расположение Internet Explorer:

– IE8-9: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\ IEDownloadHistory\;

– IE10-11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\ WebCacheV*.dat.

Загрузки включают в себя следующие данные:

– имя файла, размер и тип;
– страницу, с которой был скачен файл;
– директорию сохраненного файла;
– приложение, используемое для открытия файла;
– начало и окончание загрузки.

ADS Zone.Identifer

Начиная с ОС XP SP2, загруженные файлы из «ADS Zone» через браузер в файловую систему NTFS, создают дополнительный поток данных, который добавляется в файл. Альтернативный поток данных имеет имя «ADS Zone.Identifer».

Описание ADS Zone.Identifer:

– URLZONE_TRUSTED = ZoneID = 2;
– URLZONE_INTERNET = ZoneID = 3;
– URLZONE_UNTRUSTED = ZoneID = 4.

Например, файлы с «ADS Zone.Identifer» и содержат ZoneID=3 были загружены из сети «Интернет».

Исполнение программ. Исполнение с рабочего стола

Программы с графическим интерфейсом, которые запускались с рабочего стола, отслеживаются лаунчером ОС Windows.

Расположение ADS Zone.Identifer:

– NTUSER.DAT HIVE;

– NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count.

Характеристики ADS Zone.Identifer:

Следует отметить, что все значения ROT-13 закодированы.

Идентификатор GUID для XP:

– 75048700 – активный рабочий стол.

Идентификатор GUID для Win7/8/10:

– исполняемый файл CEBFF5CD;
– F4E57C4B файл ярлыка исполнения.

Последнее открытие MRU

В ключе OpenSaveMRU описаны последние исполняемые файлы. Также отслеживаются каталоги, которые использовались приложением для открытия последнего исполняемого файла. К примеру: последний запуск Notepad.exe был выполнен по каталогу C:\%USERPROFILE%\Desktopfolder.

Расположение MRU:

– XPNTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU;

– Win7/8/10NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU.

Описание MRU:

Отслеживаются исполняемые файлы приложений, использующие для открытия директорию OpenSaveMRU, и последний путь.

RunMRU Пуск –> Выполнить

При выполнении программы через «Пуск» – «Выполнить» создается соответствующая запись в журнале.

Расположение MRU:

– NTUSER.DAT HIVE;

– NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.

Описание MRU:

Порядок, в котором команды выполняются, перечислены в списке значений RunMRU. Буквы означают порядок, в котором команды были выполнены.

Совместимость приложений (исполняемых файлов)

Базы данных совместимости Windows используется ОС для выявления возможных проблем совместимости приложений с исполняемыми файлами.

Описание приложений (исполняемых файлов):

Отслеживаются следующие параметры исполняемых файлов: имя; размер; время последнего изменения; последние обновления (Windows XP).

Любой исполняемый файл, запущенный в ОС Windows, может быть найден в указанных разделах реестра. Можно использовать этот ключ для идентификации систем или конкретных программ, которые запускались на компьютере. Также по временным данным можно определить последнее время исполнения программ или активности в системе.

В Windows XP содержится порядка 96 записей, в том числе сведения об обновлениях системы.

Windows 7 содержит 1 024 записи.

Расположение приложений (исполняемых файлов):

– XPSYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility;

– Win7/8/10SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache.

Списки переходов (jump lists)

Панель задач Windows 7 организована так, чтобы пользователи могли выбирать пункты, которые использовались часто или недавно. Это относится не только к мультимедийным файлам, но и к последним выполняемым задачам. Данные, хранящиеся в файле AutomaticDestinations, будут иметь уникальный идентификатор AppID связанного приложения.

Расположение jump lists:

– Win7/8/10 C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations.

Описание jump lists:

Время выполнения приложения:

– время создания - первый элемент файла AutomaticDestinations;
– время изменения - последний элемент файла AutomaticDestinations.

Список переходов List IDs – http://www.forensicswiki.org/wiki/List_of_Jump_-List_IDs.

Windows Prefetch

Повышает производительность системы путем предварительной загрузки кодовых страниц часто используемых приложений. Диспетчер кэша (файл с расширением «.pf») отслеживает все запускаемые файлы и службы со ссылкой на соответствующие каталоги для того, чтобы знать какие процессы исполнялись в системе.

ОграниченияWindows Prefetch:

– 128 файлов на XP и Win7;
– 1 024 файла на Win8.

РасположениеWindows Prefetch:

– WinXP/7/8/10C:\Windows\Prefetch.

Описание Windows Prefetch:

Windows Prefetch отслеживает следующие параметры:

– время создания файла;
– количество раз запуска программ;
– путь выполнения файла;
– последнее исполнение файла;
– на Win8 содержатся последние 8 записей об исполнении.

Amacache.hve/RecentFileCache.bcf

ProgramDataUpdater использует файл реестра RecentFileCache.bcf для сохранение данных при реализации процесса.

Расположение Amacache.hve/RecentFileCache.bcf:

– Win7/8/10C:\Windows\AppCompat\Programs\Amcache.hve (Windows 7/8/10);
– Win7C:\Windows\AppCompat\Programs\RecentFilecache.bcf.

Описание Amacache.hve/RecentFileCache.bcf:

– RecentFileCache.bcf – содержит путь к исполняемому файлу и программе;
– Amcache.hve\Root\File\{Volume GUID}\####### – ключи;

– в файле $StandardInfo содержится информация о каждом запуске программы: путь, время последнего изменения и объем диска;

– SHA1 (значение хеша) исполняемого файла также содержится в ключе.

Открытие файла/папки. Открытие/сохранение MRU

Данный ключ содержит файлы, которые были созданы или сохранены в диалоговом окне оболочки Windows. Он включает в себя большой набор данных: веб-браузеры, такие как Internet Explorer и Firefox, а также большинство часто используемых приложений.

Расположение MRU:

– XPNTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\-ComDlg32\OpenSaveMRU;

– Win7/8/10NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU.

Описание MRU:

– «.*» – этот подраздел содержит самые последние файлы любого расширения (диалоговое окно Open/Save);

– «.???» – подраздел хранит информацию о файлах конкретных расширений.

Последнее посещение MRU

Данный ключ отслеживает информацию о том, с помощью каких приложений открывались те или иные файлы. Также отслеживается путь (месторасположение) файла, который был открыт приложением. Например, файл «Notepad.exe» был выполнен через путь C:\Users\Rob\Desktop folder.

Расположение последнего посещения MRU:

– XPNTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ ComDlg32\ LastVisitedMRU;

– Win7/8/10NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ ComDlg32\ LastVisitedPidlMRU.

Описание последнего посещения MRU:

Отслеживаются исполняемые приложения и их месторасположения.

Последние файлы

Ключ реестра, который отслеживает последние открытые файлы и папки, и заполняет данными папку «Recent» меню «Пуск».

Расположение последних файлов:

– NTUSER.DAT;

– NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ RecentDocs.

Описание последних файлов:

RecentDocs – ключ отслеживает порядок выполнения или открытия последних 150 файлов или папок. Также присваиваются временные метки (хронологический порядок). Последняя запись и время изменения этого ключа будет соответствовать последнему исполняемому файлу.

«.???» – данный раздел хранит последние файлы определенных расширений, которые были открыты. Также присваиваются временные метки (хронологический порядок).

Последняя запись и время изменения этого ключа будет соответствовать последнему исполняемому файлу конкретного расширения.

Folder – данный раздел хранит информацию о последних папках, которые были открыты. Также присваиваются временные метки (хронологический порядок). Последняя запись и время изменения этого ключа будет соответствовать последней открытой папке.

Последние файлы Office

Программы MS Office отслеживают собственный список недавних файлов, чтобы пользователям было легче их редактировать.

Расположение последних файлов Office

NTUSER.DAT\Software\Microsoft\Office\VERSION:

- 14.0 = Office 2010;
- 12.0 = Office 2007;
- 11.0 = Office 2003;
- 10.0 = Office XP.

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU:

- 15.0 = Office 365.

Описание: отслеживаются последние файлы, исполняемые программой MS Office. Последняя запись добавляется в MRU с указанием временной отметки.

Ключ Shell Bags

В данном ключе можно просмотреть информацию о папках, к которым были обращения по локальной сети или со съемных устройств. Также имеются следы существования удаленных или измененных папок, а также история обращений к таким папкам.

Расположение ключа

Explorer Access:

- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags;
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\ Shell\BagMRU\.

Desktop Access:

- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU;
- NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags.

Описание: ключ Shell Bags содержит данные о папках, к которым были обращения со стороны пользователей и файлы ярлыков (LNK). Раздел содержит информацию:

- о ярлыках, автоматически созданных ОС;
- о последних открытых файлах;
- об открытии удаленных файлов и файлов по локальной сети.

Ключ Recent

Расположение ключа Recent:

XP:

- C:\%USERPROFILE%\Recent.

Win7/8/10:

- C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\;
- C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\.

Следует обращать внимание на то обстоятельство, что в ключах содержится информация о первоначальных местах расположения ярлыков (могут быть и другие места).

Описание Recent:

– дата и время первого открытия файла;
– дата и время последнего открытия файла;
– дата и время создания ярлыка;
– дата и время последнего изменения ярлыка.

LNKTarget файл:

– система;
– месторасположение файла;
– изменения файла;
– наименование, тип, серийный номер;
– сетевая информация.

Windows Prefetch

Панели задач ОС Windows позволяют пользователям получать быстрый доступ к элементам часто или недавно использованным. Также содержится информация о последних выполненных задачах. Данные, содержащиеся в файле AutomaticDestinations, имеют свой уникальный идентификатор AppID в соответствии с использованными приложениями и ярлыки открытых файлов.

Расположение Windows Prefetch:

– Win7/8/10C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations.

Описание Windows Prefetch: списки переходов можно просмотреть через файлы AutomaticDestinations. Каждый из таких файлов представляет из себя ярлык (lnk) или набор цифровых данных, а именно 1 – ранее значение, наибольшее число – последнее значение.

IE|Edge file

Мало кто знает, что история интернет-браузера IE содержит в себе не только просмотр интернет-страниц, но и записи о файлах, которые появлялись в системе через съемные устройства или сетевые ресурсы. Данное обстоятельство предоставляет отличный инструмент для исследования системы.

Расположение Internet Explorer и IE|Edge file

Internet Explorer:

– IE6-7%: USERPROFILE%\Local Settings\History\ History.IE5;
– IE8-9%: USERPROFILE%\AppData\Local\Microsoft\Windows\History\.

History.IE5:

– IE10-11%: USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\ WebCacheV*.dat.

Описание IE|Edge file: файлы index.dat хранятся в директории ///C:/directory/filename.ext. IE отслеживает перемещения файлов, но это не значит, что данные файлы были открыты с помощью браузера.

Удаленные файлы

В ОС XP имеется поисковый помощник, который позволяет более эффективно находить информацию. Поисковая система «вспомнит» некоторые критерии и условия поиска такие как имя файла, тип или слова, находящиеся в содержимом файла и т. п.

Расположение удаленных файлов:

– NTUSER.DAT HIVE;

– NTUSER.DAT\Software\Microsoft\SearchAssistant\ACMru\####.

Описание удаленных файлов:

Интернет – история – ####=5001.

Имя файла или часть имени – ####=5603.

Слово или фраза в файле – ####=5604.

Принтеры, компьютеры и другие устройства – ####=5647.

Поиск по Word Wheel Query (запросу)

Ключевые слова можно искать через меню Пуск на ОС Wndows 7.

Расположение:

– Win7/8/10 NTUSER.DAT Hive;

– NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ WordWheelQuery.

Описание: ключевые слова добавляются в Unicode и перечисляются во временном порядке в MRUlist.

Последнее посещение MRU

Данный ключ отслеживает информацию о том, какие файлы какими приложениями открывались. Также отслеживается путь (месторасположение) файла, который был открыт приложением. Например, файл «Notepad.exe» был выполнен через путь C:\Users\Rob\Desktop folder.

Расположение:

XP:

– NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ LastVisitedMRU.

Win7/8/10:

– NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ LastVisitedPidlMRU.

Описание: отслеживаются исполняемые приложения и их месторасположения.

Файл Thumbs.db

Скрытый файл в каталоге, где хранится изображение на компьютере, представляющий из себя уменьшенный эскиз. При этом он сохраняется даже в случае удаления файла.

Расположение:

– WinXP/Win8|8.1: создается автоматически в любом месте.

– Win7/10: создается автоматически в любом месте и доступ к нему можно получить как локально, так и удаленно (через UNC).

Описание: файлы Thumbs.db включают в себя уменьшенное изображение исходного изображения; копию документа (даже при удалении); последнее изменение времени (только для XP); исходное имя файла (только для XP).

Данные Thumbscache

На ОС Vista/Win7 Thumbs.db не существует. Данные находятся в одном каталоге отдельно для каждого пользователя.

Расположение данных thumbscache:

– C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer.

Описание данных thumbscache: файлы создаются, когда пользователь переключал папки в режиме эскизов или просмотр фотографий через слайд-шоу. Данные хранятся в отдельной базе данных. ОС Win7 имеет 4 размера для миниатюр, и файлы в папке cache отражают это:

– 32 – > малый;
– 96 – > средний;
– 256 – > большой;
– 1024 – > очень большой.

В thumbscache будут храниться миниатюры графических файлов, размер и содержание которых эквивалентно базе данных.

Удаленные данные ОС Windows XP

Для расследования компьютерных инцидентов очень важно понимать расположение удаленных файлов. В некоторых случаях достаточно просмотреть «Корзину» или информацию о том, какие файлы там были даже после удаления их специальной программой.

Расположение удаленных данных ОС Windows XP: скрытые папки и директории

Windows XP:

– C:\RECYCLER” 2000/NT/XP/2003.

Папки создаются автоматически с работой пользователя.

Скрытый файл имеет название «INFO2» и содержит время удаления и оригинальное название файла. Наименование файлов имеет форматы UNICODE и ASCII.

Описание удаленных данных ОС Windows XP: SID может быть сопоставлен с пользователем с помощью анализа реестра. Имеется информация о имени файла и пути, по которому он был удален.

Удаленные данные ОС Windows 7/8/10

Для расследования компьютерных инцидентов очень важно понимать расположение удаленных файлов. В некоторых случаях достаточно просмотреть «Корзину» или информацию о том, какие файлы там были даже после удаления их специальной программой.

Расположение удаленных данных ОС Windows 7/8/10: скрытые папки и директории

Win7/8/10:

– C:\$Recycle.bin.

Время удаления и оригинальное имя содержатся в отдельных файлах в соответствии с удаленными файлами.

Описание удаленных данных ОС Windows 7/8/10: SID может быть сопоставлен с пользователем с помощью анализа реестра.

Win7/8/10: содержимому файлов предшествует $|######. Имеется информация о пути файла, времени удаления и наименовании. Содержимому восстановленных файлов предшествует $R######.

IE|Edge file

Мало кто знает, что история интернет-браузера IE содержит в себе не только просмотр интернет-страниц, но и записи о файлах, которые появлялись в системе через съемные устройства или сетевые ресурсы. Данное обстоятельство предоставляет отличный инструмент для исследования системы.

Расположение IE|Edge file:

Internet Explorer:

– IE6-7: %USERPROFILE%\Local Settings\History\ History.IE5;

– IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\History\.

History.IE5:

– IE10-11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\ WebCacheV*.dat.

Описание IE|Edge file: файлы index.dat хранятся в директории ///C:/directory/filename.ext. IE отслеживает перемещения файлов, но это не значит, что данные файлы были открыты с помощью браузера.

ГЛАВА IV. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ И УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ ВОПРОСЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ ПРОТИВ СОБСТВЕННОСТИ

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

В настоящее время нет общепризнанного определения понятие преступлений в сфере компьютерной информации, совершаемых против собственности, соответственно отсутствует соответствующая статистика. Однако в ведомственной статистике МВД России, есть показатели количества преступлений в сфере компьютерной информации (в 2019 г. зарегистрировано 2 883) и преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий (в 2018 г. зарегистрировано 174 674)[1]. В 2019 г. зарегистрировано уже 294 409 тыс. (+ 68,5 % к АППГ) преступлений, совершенных с использованием информационно-телекоммуникационных технологий (далее – ИТТ).

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

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

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

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

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

Наиболее распространенными способами совершения таких преступлений являются:

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

– неправомерный доступ к охраняемой законом компьютерной информации;

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

---

[1] Состояние преступности в Российской Федерации за январь–декабрь 2019 г. // URL: https://мвд.рф/reports /item/.

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

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

Следует отметить, что по итогам девяти месяцев 2019 г. раскрываемость преступлений в рассматриваемой группе составила всего 27,1 %. По нашему мнению, одной из причин данных низких показателей является несовершенство работы следователей (дознавателей) на стадии возбуждения уголовного дела.

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

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

В соответствии с ч. 1 ст. 140 УПК РФ поводами для возбуждения уголовного дела служат:

– заявление о преступлении;

– явка с повинной;

– сообщение о совершенном или готовящемся преступлении, полученное из иных источников;

– постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании.

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

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

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

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

Следует помнить, что в уголовно-процессуальном законе отсутствует требование об обязательности выяснения уже на стадии возбуждения уголовного дела всех обстоятельств происшедшего события, содержащего признаки преступления. На данной стадии достаточно установить факты, указывающие на наличие признаков преступле-

---

[1] Информационно-аналитические материалы Следственного департамента МВД России за 2017 г.

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

ния, выяснение же конкретных обстоятельств преступления и лиц, виновных в его совершении, возможно после возбуждения уголовного дела в ходе предварительного расследования[1].

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

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

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

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

В последнее время, при совершении преступлений в сфере компьютерной информации, совершаемых против собственности, все чаще используются методы социальной инженерии[2] в системах дистанционного банковского обслуживания (далее – ДБО).

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

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

– способ подготовки, совершения и сокрытия хищения;

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

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

– сведения о лицах, причастных к хищению (ФИО, имена учетных записей в программах для мгновенного обмена сообщениями, IP-адреса, данные из социальных сетей, почтовые адреса, и т. д.);

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

---

[1] Обзор судебной практики Верховного Суда Российской Федерации № 3, 2017 (утв. Президиумом Верховного Суда Российской Федерации 12 июля 2017 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru» (дата обращения: 07.11.2019).

[2] Социальная инженерия – это общность приемов, методов и технологий создания определенного пространства, условий и обстоятельств, которые могут привести к получению конфиденциальной информации, с использованием социологии и психологии. Основная цель социальной инженерии получение доступа к защищенным системам, к примеру, злоумышленники могут получить доступ к паролям и банковским данным человека. Сложность противодействия подобным преступлениям заключается в том, что все действия со стороны жертвы финансового преступления совершаются добровольно.

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

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

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

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

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

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

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

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

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

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

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

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

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

– протокол осмотра места происшествия;

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

– рапорт сотрудника об обнаружении признаков преступления;

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

Следует отметить, что для стадии возбуждения уголовного дела по преступлениям в сфере компьютерной информации, совершаемым против собственности при производстве процессуальных действий, предусмотренных ч. 1 ст. 144 УПК РФ характерно участие специалиста. Так, при осмотре места происшествия, опросе киберпреступников, назначении компьютерно-технической экспертизы, осмотре и исследовании предметов и документов участие специалиста позволит обеспечить необходимое качество проведения данных процессуальных действий и позволит предотвратить утрату важной доказательственной информации. Среди высококвалифицированных специалистов выделяют[2]:

---

[1] Информационно-аналитические материалы Следственного департамента МВД России за 2015 г.

[2] В основном это специалисты, работающие в области информационных технологий и осуществляющие защиту информации, которую охраняет закон. К охраняемой законом информации относятся: государственная, военная и служебная тайна; служебная информация; нотариальная тайна; инсайдерская информация; персональные данные; профессиональная и коммерческая тайна; банковская тайна (ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности») и тайна кредитной истории (ст. 7 Федерального закона от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях»).

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

– специалистов компаний, обеспечивающих информационную безопасность (Лаборатория Касперского, Group-IB, BI.ZONE, Positive Technologies и др.);

– специалистов, выполняющих судебные компьютерно-технические экспертизы;

– работников службы информационной безопасности различных организаций и учреждений;

– сотрудники научно-исследовательских и учебных заведений соответствующего профиля.

Следует указать, что в ходе уголовного дела обязательно проведение экспертизы. Предметом экспертизы будут изъятые по делу электронные носители информации, ноутбуки, флэш-карты и т. д. Цель – обнаружить вредоносное программное обеспечение на тех или иных сведениях, имеющих значение для выявления признаков преступления (однако ст. 196 УПК РФ не содержит требование обязательности назначения экспертиз по делам данной категории, но данное требование обусловлено процессом доказывания по такого рода делам).

Здесь нужно обратить внимание на те случаи, когда отсутствует заявление со стороны пострадавших. Между тем, лицо может даже не подозревать, что в отношении его была попытка совершить хищение денежных средств, с помощью информационных технологий. Например, внедренное преступниками вредоносное программное обеспечение подменило платежные реквизиты в осуществляемой транзакции, однако система «Фрод-мониторинга» и сотрудники службы безопасности финансово-кредитной организации заблокировали данную транзакцию. В подобных случаях, атакуемое лицо даже не подозревает, что сотрудники кибербезопасности кредитной организации предотвратили хищение его денежных средств, что исключает личное обращение в правоохранительные органы. В свою очередь сотрудники безопасности кредитной организации соблюдая требования ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» так же не могут инициативно передавать в правоохранительные органы информацию о подобных инцидентах.

Как правило, при совершении преступлений в сфере информационных технологий, отсутствуют очевидцы, так как общение преступников происходит в информационно-телекоммуникационной сети, с использованием специальных программ, обеспечивающих анонимность такой коммуникации (анонимайзеров)[1].

Киберпреступления зачастую взаимосвязаны с подготавливаемыми или уже совершенными общеуголовными преступлениями. Так, осенью 2017 г. анонимные сообщения о заложенных бомбах поступали из разных городов России: Владивостока, Магадана, Омска, Челябинска, Уфы, Перми, Ставрополя и Москвы. Основной версией по-

[1] Анонимайзер – общее название средств для скрытия информации о компьютере, его IP-адресе или пользователе в сети от удаленного сервера. Анонимайзеры применяются не только для обеспечения конфиденциальности, но и для посещения заблокированных в стране сайтов или обхода ограничений файлообменников.

добных звонков является спланированная атака с применением средств IP-телефонии[1]. Такие системы позволяют организовать массовый обзвон из одного–двух мест и при этом скрывать настоящий номер абонента[2].

К особенностям, характеризующим большинство киберпреступлений, можно отнести криминальную круговую поруку, слабую свидетельскую и доказательную базу по делам указанной категории, сложность установления и доказывания связей между различными участниками преступных групп.

Еще один момент, который следует учесть при оценке первичных материалов о противоправных деяниях в сфере компьютерной информации – это малозначительность деяния[3]. В ч. 2 ст. 14 УК РФ, закреплено, что преступлением не является действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного Уголовным кодексом, но в силу малозначительности не представляет общественной опасности.

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

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

§ 4.2. Уголовно-процессуальные основы досудебного производства по уголовным делам о преступлениях в сфере компьютерной информации, совершаемых против собственности

В последнее время, цифровые и телекоммуникационные технологии активно используются правонарушителями в целях совершения различных видов хищения.

Согласно Доктрине информационной безопасности Российской Федерации, информационная сфера определена как совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием

---

[1] IP–телефония – набор коммуникационных протоколов, технологий и методов, обеспечивающих набор номера, дозвон, двустороннее голосовое общение, а также видеообщение по сети «Интернет» или другим IP-сетям. Сигнал передается по каналу связи цифровом виде и, как правило, перед передачей преобразуется (сжимается), чтобы удалить избыточность информации и снизить нагрузку на сеть передачи данных.

[2] Ложная тревога // URL: https://rg.ru/2017/09/12/reg-pfo/v-krupnyh-gorodah-rossii-evakuirovali-desiatki-shkol-vokzalov-i-tc.html (дата обращения: 15.04.2019) ; Телефонные террористы дозвонились в Москву // URL: https://www.kommersant.ru/doc/3409928 (дата обращения: 15.01.2020).

[3] Следует обратить внимание, что деяние формально обладает признаками преступления, предусмотренного уголовным законом, но при этом деяние по своей общественной опасности ничтожно, не причинило и не создало угрозы причинения вреда общественным отношениям.

названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений[1]. При этом реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Указом Президента России утверждена «Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.»[2], которая определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов. Так, одним из основных принципов данной стратегии является обеспечение государственной защиты интересов российских граждан в информационной сфере.

Вышеперечисленные нормативные правовые акты показывают вектор развития общества, а именно переход в информационную сферу основных видов жизнедеятельности общества.

Вместе с тем в Доктрине информационной безопасности Российской Федерации констатировано, что расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы. 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.

Переход большинства общественных отношений в сферу компьютерной информации не только меняет жизнь граждан в силу стремительного развитии экономики и других социальных сфер жизни общества, но и привлекает внимание лиц, которые заинтересованы в незаконном получении доходов. За последние пять лет отмечается неуклонный рост преступлений в сфере информационных технологий (в том числе преступлений в сфере компьютерной информации, совершаемых против собственности). Так, с 2015 г. по 2019 г. число зарегистрированных преступлений ежегодно увеличивается минимум на 50 %[3].

---

[1] Указ Президента Российской Федерации от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» № 646 // СПС «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 10.01.2020).

[2] Указ Президента Российской Федерации от 9 мая 2017 г. «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.» № 203 // СПС «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 10.01.2020).

[3] В 2015 г. зарегистрированы 43 816 преступлений в сфере информационных технологий, в 2016 г. – 65 949 преступлений, а в 2019 г. – 294 409 преступлений.

Таким образом, очевидно, что система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Если рассматривать преступления в сфере компьютерной информации, совершаемые против собственности, то статистика показывает значительный рост выявленных преступлений, предусмотренных ст.ст. 158 и 159 УК РФ. Так, в 2016 г. выявлены 9 762 преступления, предусмотренных ст. 158 УК РФ, связанных с применением информационных технологий, что на 15,5 % больше, чем аналогичный показатель 2015 г. Количество мошенничеств в сфере компьютерной информации, совершенных против собственности, в 2016 г. выросло на 143,5 % по сравнению с 2015 г.[1]

В 2018 и 2019 гг. число преступлений, связанных с использованием информационных технологий, не только не уменьшилось: Генеральный прокурор России отметил, что за 2018 г. произошел двукратный рост IT-преступлений по сравнению с 2017 г.[2] За 9 месяцев 2019 г. увеличение таких преступлений составило почти 70 % (69,2 %) по сравнению с аналогичным периодом 2018 г.[3]

Рассматривая приведенные статистические данные, можно сделать вывод о том, что с развитием информатизации общества увеличиваются как количественные (становится больше зарегистрированных преступлений), так и «качественные»[4] показатели преступности с использованием информационных технологий.

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

Очевидно, в силу единства уголовно-процессуальной формы производство по уголовным делам о преступлениях в сфере компьютерной информации, совершаемых против собственности, подчиняется общим правилам, тем не менее, доказывание обстоятельств указанных преступлений все же обладает определенной спецификой, прежде всего в части особенностей предмета доказывания.

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

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

---

[1] Аналитический обзор практики расследования преступлений Следственного департамента МВД России в сфере информационных технологий по итогам 2016 г.

[2] Доклад Генерального прокурора Российской Федерации Ю. Чайки на заседании Совета Федерации Федерального Собрания Российской Федерации // URL: http://www.procrf.ru/news/734623-doklad-generalnogo-prokurora-rf.html (дата обращения: 10.01.2020).

[3] Решение коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3.

[4] Рассматриваемые преступления совершаются технически оснащенными, еще лучше законспирированными преступными группами, в том числе международными, характеризуются усложненными способами подготовки их совершения и сокрытия, созданием и использованием все более совершенных вредоносных компьютерных программ.

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

– обстоятельства, характеризующие личность обвиняемого;

– характер и размер вреда, причиненного преступлением;

– обстоятельства, исключающие преступность и наказуемость деяния;

– обстоятельства, смягчающие и отягчающие наказание;

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

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

– обстоятельства, способствовавшие совершению преступления.

При производстве по уголовным делам о преступлениях в сфере компьютерной информации, совершаемых против собственности, должны быть установлены все перечисленные обстоятельства, однако наибольшая специфика присуща доказыванию обстоятельств, закрепленных в п. 1 ч. 1 ст. 73 УПК РФ – «событие преступления» и в п. 2 ч. 1 ст. 73 УПК РФ – «виновность лица в совершении преступления».

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

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

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

Для написания сложных компьютерных программ, которые планируется использовать при совершении нескольких преступлений, привлекается группа специалистов-

[1] Вредоносная компьютерная программа – это любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации / URL: http://www.ruukrf.ru (дата обращения: 10.01.2020).

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

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

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

В связи с этим для определения времени создания вредоносной компьютерной программы необходимо:

– установить место, где она была создана;

– синхронизировать время, установленное на ЭВМ, с реальным временем;

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

Исходя из этого, по уголовным делам о преступлениях в сфере компьютерной информации, совершаемых против собственности, время совершения преступления должно пониматься в широком смысле и включать в себя:

– время приискания лиц и средств для изготовления вредоносного программного обеспечения;

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

– время начала использования вредоносной программы;

– время фактического использования указанной программы для получения выгоды.

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

---

[1] Всестороннее исследование проблемы киберпреступности // Управление Организации Объединенных Наций по наркотикам и преступности / Vienna International Centre, PO Box 500, 1400. Vienna, Austria.

[2] Компиляция – трансляция программы, составленной на исходном языке высокого уровня, в эквивалентную программу на низкоуровневом языке, близком машинному коду (абсолютный код, объектный модуль, иногда на язык ассемблера). Другими словами – процесс перевода из программного кода в программу, используемую ЭВМ // URL: http://www.ruukrf.ru (дата обращения: 10.01.2020) ; Компиляция / Информационный портал «Языки программирования» // URL: http://programming-lang.com (дата обращения: 10.01.2020).

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

2. Место совершения преступления. Понятие места совершения преступления на законодательном уровне не закреплено, однако, общепризнанно, что под местом совершения преступления следует понимать, территорию на которой совершается преступление[1].

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

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

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

Надо отметить, что термин «территория» является условным понятием при расследовании уголовных дел о преступлениях в сфере компьютерной информации. В глобальной сети «Интернет» все чаще используется понятие «сегментов»[2]. Для определения территории, где было совершено то или иное преступление, необходимо установить «веб-сервер»[3], на котором расположен определенный сайт[4]. Таким образом, с помощью «веб-серверов» и другого программного обеспечения преступления в сфере компьютерной информации могут быть начаты на территории одного государства, а продолжены и окончены на территории других.

Исходя из вышеизложенного, понятие места совершения преступления в классическом виде не всегда применимо в полной мере при доказывании обстоятельств преступлений в сфере компьютерной информации, совершаемых против собственности.

---

[1] Российской уголовное право. Общая часть : учебник / под ред. Л. В. Иногамовой-Хегай [и др.]. М., 2010. С. 42.

[2] Сегмент интернета – это часть сайтов в глобальной сети «Интернет» с основным контентом (содержанием) на одном языке. Так, «Рунет» – часть сайтов Интернета с основным контентом на русском языке ; Основы сетевых технологий : учебник для вузов / Н. А. Руденков, Л. И. Долинер. Екатеринбург : Уральский Федеральный университет, 2011. 300 с.

[3] Сервер (от англ. «server», to serve – служить) – специализированный компьютер и/или специализированное оборудование для выполнения на нем сервисного программного обеспечения (в том числе серверов тех или иных задач). Веб-сервер – специализированный компьютер для выполнения различных задач в глобальной сети «Интернет».

[4] Степанов А. Н. Информатика для студентов гуманитарных специальностей. 3-е изд. СПб. : Питер, 2002. 608 с.

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

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

При расследовании уголовных дел о преступлениях в сфере компьютерной информации, совершаемых против собственности, территориальная подследственность должна определяться территориальным нахождением организации (юридический адрес) кредитно-банковской сферы, на счет которой преступник перечислил похищенные денежные средства. Однако ни само лицо, совершившее преступление, ни потерпевший могут фактически не иметь к указанной территории никакого отношения.

Отмечая данную проблему, в июне 2014 г. Следственным департаментом МВД России в органы предварительного следствия направлены директивные указания (№ 17/3-16230 от 20 июня 2014 г.) об исключении необоснованного перенаправления в порядке ст. 152 УПК РФ материалов доследственной проверки о преступлениях рассматриваемой категории, влекущего увеличение сроков ее проведения и утрату следов преступления, необходимости, при наличии достаточных оснований, принимать процессуальное решение о возбуждении уголовного дела по месту поступления заявления о совершенном преступлении.

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

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

Рассматривая вопрос о месте совершения преступления, нужно учитывать ранее обозначенное обстоятельство, что преступления в сфере компьютерной информации, совершаемые против собственности, включают в себя несколько этапов преступной деятельности, в связи с чем необходимо установить:

- место или места написания программного кода вредоносной программы;
- место компиляции указанной программы;
- место нахождения объекта преступного посягательства.

При установлении места, где осуществлялось написание программного кода вредоносной программы, и места, где производилась компиляции данной программы, необходимо определить: во-первых, фактический адрес расположения ЭВМ, на которой осуществлялись указанные действия; во-вторых, место осуществления доступа к глобальной сети «Интернет»; в-третьих, место подключения к локальным сетям общего пользования или закрытым локальным сетям; в-четвертых, идентификационные номера компьютера (IP-адресов, MAC-адреса сетевого оборудования и других).

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

Таким образом, при установлении места совершения преступления необходимо устанавливать не только фактическое место нахождения организации, откуда были похищены денежные средства, место нахождения ЭВМ, на которых был написан программный код вредоносной программы и на котором осуществлялась компиляция указанной программы, а также их «электронный адрес», т. е. адрес в глобальной сети «Интернет».

При доказывании преступлений в сфере компьютерной информации, совершаемых против собственности, надо учитывать тот факт, что часто определить место совершения преступных деяний невозможно.

Примером данных случаев будут служить те факты, когда злоумышленники в своей преступной деятельности используют возможности сегмента глобальной сети «Интернет» «.onion»[4] или возможности интернет-ресурсов так называемого «ДаркНета»[5].

---

[1] Доменный адрес или домен – символьное имя, служащее для идентификации областей – единиц административной автономии в сети «Интернет» (в составе вышестоящей по иерархии такой области), т. е. домен – это адрес в глобальной сети «Интернет».

[2] IP-адрес – это уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP. Другими словами – это номер ЭВМ (сети ЭВМ), который присваивается поставщиком услуг, обеспечивающим доступ в глобальную сеть «Интернет».

[3] MAC-адрес (от англ. Media Access Control – управление доступом к среде; Hardware Address) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Интернет. MAC-адрес – это уникальный номер элемента компьютера, обеспечивающего возможность подключения к сети, в том числе и к глобальной сети «Интернет».

[4] .onion – псевдодомен верхнего уровня (схожий по применению с доменами «.bitnet» и «.uucp», использовавшимися ранее), созданный для обеспечения доступа к анонимным или псевдоанонимным адресам сети Tor (сокр. от англ. The Onion Router). Подобные адреса не являются полноценными записями DNS, и информация о них не хранится в корневых серверах DNS, но при установке дополнительного программного обеспечения, необходимого для выхода в сеть Tor (например, Orbot для Android или плагин Torbutton для Firefox), программы, работающие с Интернетом, получают доступ к сайтам в доменной зоне «.onion», посылая запрос через сеть Tor-серверов // Мониторинг Реестра запрещенных сайтов: статистика / URL: https://antizapret.info/index.php?search=onion.to (дата обращения: 10.01.2020) ; Романова А. С. Борьба с преступностью в компьютерных сетях «глубинного» интернета / Материалы всероссийской научно-практической конференции «Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования». Иркутск : Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2016. С. 122–127.

[5] Даркнет (от англ. DarkNet) – частная сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов // TOR : a Dark Net Journey on How to Be Anonymous Online (TOR, Dark Net, DarkNet, Deep web, cyber security Book / John Smith. North Charleston (SC) : CreateSpace Independent Publishing Platform, 2017. 50 с. ; Фролов А. А., Сильнов Д. С. Исследование механизмов рассмотрения, запрещенного содержимого в DARKNET / Международный научный журнал «Современные информационные технологии и ИТ-образование». – 2017. – № 4. – С. 216–224.

Данный сегмент Интернета не имеет фактической привязки к физическим адресам, поэтому местом совершения преступления будет являться «электронный» (доменный) адрес в глобальной сети «Интернет».

Исходя из этого, можно сделать вывод, что местом совершения преступлений в сфере компьютерной информации, в т. ч. против собственности, может являться как физический адрес нахождения объекта преступления, так и электронный адрес места нахождения ресурса, способствующему совершению преступления, который не имеет фактической привязки к физическому адресу, либо физический адрес указанного ресурса вообще невозможно установить.

3. Способ совершения преступления. Процесс доказывания способа совершения компьютерных преступлений – один из самых сложных, это обусловлено тем, что преступник постоянно пытается скрыть свои действия, а современные технические и технологические возможности и глобализация лишь способствуют этому.

Исходя из гл. 28 УК РФ «Преступления в сфере компьютерной информации», по способам совершения компьютерных преступлений выделяют деяния:

– связанные с изъятием компьютерной информации;
– связанные с перехватом информации;
– связанные с несанкционированным доступом;
– связанные с манипуляцией информацией и ее подменой;
– совершенные комплексными способами[1].

Данная классификация мало применима к преступлениям, связанным с хищением денежных средств.

Так, на первоначальном этапе расследования следователю известно лишь место фактического совершения преступного деяния, причиненный ущерб и личность потерпевшего. После установления данных фактов следующим вопросом, который будет требовать разрешения, является именно способ совершения преступления.

Исходя из этого, следователь должен определить, каким способом было произведено «заражение» вредоносным программным обеспечением. И исходя из этого, складываются две основные следственные ситуации, обусловленные способами совершения преступления:

– вредоносным программным обеспечением заражена непосредственно ЭВМ, которая производила операции. Это могут быть ситуации, когда злоумышленники при помощи вредоносного программного обеспечения получали доступ к сервисам «онлайн Банка», к личным данным, позволяющим совершить хищение, и т. д.;

– вредоносным программным обеспечением заражена ЭВМ, которая выполняла обработку операции. Здесь нужно отметить, те случаи, когда преступники «заражали» ЭВМ организаций, предоставляющих услуги населению в кредитной и банковской сфере[2].

---

[1] Тер-Акопов А. А. Преступление и проблемы нефизической причинности в уголовном праве : монография / А. А. Тер-Акопов. М. : Юркнига, 2003. 480 с. ; Арзамасцев М. В. К вопросу об уголовно-правовой классификации киберпреступлений / Актуальные вопросы права и отраслевых наук. – 2017. – № 1 (3). – С. 11–17.

[2] Стоит отметить, что удельный вес преступлений второй группы на данный момент минимален, что во многом связано с тем, что данные учреждения тратят огромные ресурсы на обеспечение кибербезопасности.

Если установлено использование вредоносного программного обеспечения в совершении преступления, должны рассматриваться как минимум три основные версии способа совершения:

– физическое «заражение» ЭВМ (установка вредоносного программного обеспечения с различных переносных накопителей информации (карты памяти, «флеш-накопители информации», CD или DVD, цифровые устройства и т. д.);

– «заражение» ЭВМ из локальной сети (вредоносная программа может быть распространена через локальную сеть. Например, когда сотрудник организации использовал компьютер в личных целях, после чего подключился к рабочей сети и, неведомо для себя, распространил вредоносную программу);

– «заражение» ЭВМ из глобальной сети «Интернет» – это самый распространенный случай, а способы его реализации могут быть различными и постоянно совершенствуются злоумышленниками. К ним можно отнести рассылку вредоносного программного обеспечения в социальных сетях или по электронной почте, создание дубликатов сайтов («фишинг») и т. д.

В процессе доказывания способа совершения указанных видов преступлений необходимо определить место нахождения вредоносного программного обеспечения в момент совершения хищения. Затем нужно определить способы «заражения» вредоносным программным обеспечением. Далее необходимо установить источник, от которого произошла передача вредоносного программного обеспечения. При установлении данных фактов на заключительном этапе доказывания необходимо определить все пути распространения вредоносного программного обеспечения и установить «первоисточник». «Первоисточником» будет считаться ЭВМ, на которой было скомпилировано вредоносное программное обеспечение, или на котором находилась его копия в момент начала реализации преступного умысла. Стоит отметить, что злоумышленники, с целью сокрытия своего места нахождения, часто пользуются программным обеспечением, которые изменяет или скрывает привязку к физическому адресу. Собирание доказательств, направленных на установление факта использования таких программ, имеет значение и для установления способа совершения преступления.

Таким образом, при определении способа совершения преступлений в сфере компьютерной информации, совершаемых против собственности, необходимо установления местонахождения вредоносного программного обеспечения в момент совершения хищения, способа «заражения», установления пути распространения от злоумышленника до потерпевшего.

Установление указанного в п. 2 ч. 1 ст. 73 УПК РФ обстоятельства, входящего в предмет доказывания по уголовным делам о преступлениях в сфере компьютерной информации, совершаемых против собственности («виновность лица в совершении преступления») неизбежно связано с установлением события данного преступления.

Примером может служить уголовное дело в отношении братьев Дмитрия и Евгения Попелышей[1]. В ходе расследования данного уголовного дела было установлено время совершения преступления: время компиляции и начала использования вредоносного программного обеспечения (программы семейства «Trojan.Win32.VKhost»), время со-

[1] Дело о фишинге: как ловили хакеров-близнецов из Санкт-Петербурга // URL: https://ria.ru/incidents/20121221/915789715.html (дата обращения: 10.01.2020).

здания «фишинговых» сайтов, имитирующих страницы ВТБ 24 и Телебанка, а также время фактического хищения денежных средств. Следователям удалось установить доменный адрес и выяснить, что братья привлекли к своей преступной деятельности Александра Сарбина, который помогал братьям осуществлять хищения, создавая поддельные страницы веб-банкинга банка ВТБ 24 и серверную инфраструктуру. Однако уголовное дело было возбуждено в январе 2011 г. по признакам состава преступления, предусмотренного ч. 1 ст. 273, ч. 3. ст. 30 и ч. 4 ст. 159 УК РФ, а первое рассмотрение дела состоялось в мае 2012 г. в Петроградском районном суде Санкт-Петербурга. Позже дело было передано в Чертановский суд Москвы, где спустя несколько месяцев был вынесен обвинительный приговор. суд приговорил их к шести годам лишения свободы условно с испытательным сроком пять лет. В ходе расследования удалось доказать, что вредоносная программа «VKhost» была приобретена на черном рынке, а на компьютере, изъятом правоохранительными органами, была обнаружена среда разработки Delphi[1].

Впоследствии оказавшись на свободе, братья руководили группой программистов, которые использовали новые вредоносные программы «QHost» и «Patched.IB». В ходе совместной спецоперации ФСБ и МВД России в мае 2015 г. в Санкт-Петербурге братьев Попелышей и их подельников повторно задержали и обвинили по ст.ст. 159, 272, 273 УК РФ[2].

Для того, чтобы доказать виновность лица в совершении преступления в сфере компьютерной информации, в том числе против собственности, прежде всего, требуется установить место нахождения ЭВМ, которая использовалась в преступной деятельности. Однако установление данной вычислительной машины прямо не указывает на лицо, совершившее преступления. Для установления лица (лиц), совершивших указанные виды преступлений, зачастую необходимо произвести совокупность ни только следственных действий и оперативно-разыскных мероприятий, но привлечь к участию в них лиц, обладающих специальными знаниями (экспертов, специалистов).

С помощью оперативных мероприятий следователь получает информацию о возможной причастности лица (лиц) к совершению указанного вида преступления, после чего путем проведения следственных и иных действий доказывает указанный факт.

Однако, в большинстве случаев в результате следственных действий будет установлено два основных факта: лицо (лица) постоянно пользовались ЭВМ; данная ЭВМ использовалась в преступной деятельности. Но этого недостаточно для предъявления обвинения.

В связи с этим в рамках предварительного расследования необходимо привлечение экспертов и специалистов, которые смогут установить факт применения (изготовления) вредоносного программного обеспечения конкретным лицом. Данные действия в каждом конкретном случае являются уникальными, так как деятельность преступников не строится «по одним шаблонам» и часто носит скрытый характер.

---

[1] Delphi – среда разработки, основная область использования – написание прикладного программного обеспечения, является диалектом языка Object Pascal.

[2] 18 июня 2015 г. Савеловский суд Москвы признал вину подсудимых – Евгений и Дмитрий Попелыши получили по 8 лет лишения свободы, А. Сарбин – 6 лет // URL: https://www/group-ib.ru/blog/brothers (дата обращения: 10.01.2020).

Исходя из этого, целесообразно привлечение специалиста при производстве первоначальных следственных действиях и оперативно-разыскных мероприятий, либо передача в распоряжение эксперта, производящего компьютерную экспертизу, не только всех материалов уголовного дела, но и всех изъятых предметов и документов. Данный факт будет способствовать идентификации личности преступника и сбору доказательств, подтверждающих его виновность.

Таким образом, в рамках общих правил досудебного производства по уголовным делам о преступлениях в сфере компьютерной информации, совершаемых против собственности, положения о предмете доказывания обладают существенной спецификой, что связано с особенностями установления времени, места и способа совершения указанных преступных деяний, а также виновности лиц, их совершивших.

ГЛАВА V. ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ ПРОТИВ СОБСТВЕННОСТИ

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

Ранее приведенные статистические показатели зарегистрированных хищений в сфере информационных технологий свидетельствуют об их устойчивом росте, что связано с тенденцией увеличения преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий.

Более глубокий анализ структуры данных преступлений позволяет прийти к выводу, что именно дистанционные хищения безналичных денежных средств физических лиц, в числе которых выделяются кражи и мошенничества, занимают среди них «ядерную» часть – 85 %.

Кражи (ст. 158 УК РФ), находятся на втором месте среди всех преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий. В 2015 г. краж было зарегистрировано 8 452, в 2016 г. – 9 762, в 2017 г. только 6 945, то в 2018 г. – уже 36 167. По итогам 2019 г. количество зарегистрированных дистанционных краж возросло практически в несколько раз. Частично на эту ситуацию повлияло изменение взгляда высшего судебного органа на квалификацию данных преступлений и включение в ч. 3 ст. 158 УК РФ нового пункта «г», предусматривающего ответственность за кражу с банковского счета, а равно в отношении электронных денежных средств.

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

Дистанционные хищения безналичных денежных средств, совершаемые с использованием компьютерных и телекоммуникационных технологий, относятся к категории технически сложных по замыслу и исполнению преступлений. Для их осуществления преступники часто объединяются в группы с четким распределением ролей в процессе подготовки и реализации преступного замысла. Организаторы и исполнители нередко обладают высокой квалификацией и глубокими знаниями в области информационных технологий, психологии и в сфере банковского обслуживания клиентов. Поэтому органам внутренних дел особенно важно противопоставить их действиям своевременные и квалифицированные меры по выявлению, пресечению и предупреждению преступных посягательств в этой сфере, их разоблачению и привлечению виновных к уголовной ответственности. Так раскрытием дистанционных хищений в сфере информационных технологий, в первую очередь, занимаются подразделения уголовного розыска.

В настоящее время известно множество различных видов дистанционных хищений безналичных денежных средств физических лиц с использованием информационно-телекоммуникационных технологий. Механизм их совершения характеризуется тем, что преступники не вступают в непосредственный контакт с потерпевшими. Это значительно усложняет раскрытие и расследование таких преступлений, так как потерпевший впоследствии не может воспроизвести признаки внешности преступника. Специфика состоит еще и в том, что в отличие от преступлений, которым присущ физический способ воздействия на потерпевшего, при дистанционных хищениях в сфере информационно-телекоммуникационных технологий способ воздействия на потерпевшего носит дистанционный характер и строится на особых доверительных отношениях, сложившихся между потерпевшим и преступником благодаря умелому применению приемов социальной инженерии[1].

Представляется, что для грамотного планирования и организации раскрытия и расследования дистанционных хищений безналичных денежных средств физических лиц, совершаемых с использованием информационно-телекоммуникационных технологий, практическим сотрудникам требуется детально уяснить структуру данных преступлений, понимать механизм преступных действий, а для этого им необходимо ознакомиться с подробной классификацией современных способов их совершения. Ведь давно известно, что изучение способов совершения преступлений служит ценным источником сведений, необходимых для разработки средств, приемов и методов раскрытия, расследования и предупреждения преступлений[2].

---

[1] Социальная инженерия – это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным. В сфере информационной безопасности данный термин был популяризован в начале XXI в. бывшим компьютерным преступником, ныне консультантом по безопасности, Кевином Митником, который утверждал, что самое уязвимое место любой системы безопасности – человеческий фактор. Так одной из наиболее распространенных схем является мошенничество с использованием брендов известных корпораций. В таких фишинговых схемах используются поддельные сообщения электронной почты или веб-сайты (например, поздравления с победой в конкурсе, о срочном изменении учетных данных), содержащие названия крупных или известных компаний, злоумышленники могут проводить подобные мошеннические схемы по телефону от лица службы технической поддержки // Wikipedia.org: свободная энциклопедия. URL: https://ru.m.wikipedia.org/wiki/ Социальная_инженерия (дата обращения: 04.02.2020).

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

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

Предлагаем подробней разобрать способы совершения наиболее распространенных дистанционных хищений безналичных денежных средств у физических лиц, совершаемых в сфере информационно-телекоммуникационных технологий, по которым проведение оперативно-разыскных мероприятий осуществляется силами подразделений уголовного розыска территориальных органов внутренних дел.

В самом общем виде их можно разделить на два вида:

– дистанционные хищения безналичных денежных средств физических лиц с использованием средств мобильной телефонной связи (к примеру, телефонные кражи);

– дистанционные хищения безналичных денежных средств физических лиц с использованием сети «Интернет» (к примеру, интернет-кражи и интернет-мошенничества).

§ 5.1. Оперативно-разыскная характеристика распространенных дистанционных хищений безналичных денежных средств физических лиц, совершаемых с использованием средств мобильной телефонной связи

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

– телефонные хищения безналичных денежных средств физических лиц под видом блокировки их банковской платежной карты (далее – БПК) или несанкционированного списания с нее средств (СМС-кражи и СМС-мошенничества);

– телефонные хищения денежных средств физических лиц под видом возникших проблем с законом у их родственника;

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

Рассмотрим подробно каждый из перечисленных способов:

1. Схема телефонных хищений безналичных денежных средств физических лиц под видом блокировки их банковской платежной карты или несанкционированного списания с нее средств (СМС-кражи и СМС-мошенничества)[1]

Человек, имеющий в своем распоряжении БПК, получает СМС-сообщение, содержащее телефон для обратной связи. Наиболее распространенными вариантами таких сообщений являются:

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

– «Уважаемый клиент, с вашей банковской карты списано 9 800,60 руб. Инф. : 88005552010»;

– «Операции по вашей карте приостановлены. Обращаться по тел.: 88005553355»;

– «Оплата услуг на сумму 7 380 RUB произведена успешно. Инфо : 89512700935»;

– «Оплата покупки с вашей банковской карты на сумму 13 700 руб. успешно зарезервирована/ OZON.ru. Платеж будет проведен в течение суток. Если вы не совершали покупку, срочно свяжитесь со службой поддержки: 88005553355».

Причем в качестве телефона для обратной связи может быть указан многоканальный федеральный бесплатный номер (например, 88005550550, 88005055505, 88005505550 и др.)[2].

Человеку, перезвонившему на указанный в сообщении номер, злоумышленники представляются:

– сотрудниками службы безопасности банка;

– специалистами службы технической поддержки или контактного центра;

– сотрудниками платежной системы.

Преступники вводят человека в заблуждение и вытягивают из него информацию относительно реквизитов его банковской платежной карты.

Нередко уже на этом этапе преступники пытаются провести регистрацию (перерегистрацию) Интернет-банка потерпевшего. Для этого они в Интернете открывают

---

[1] В соответствии с ч. 3 п. 17 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» и разъяснениями, «когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража». Несмотря на это, анализ способов совершения преступлений данного вида показывает, что часто преступники не ограничиваются выяснением только лишь реквизитов БПК или персональных данных потерпевшего. Например, используя преступную схему с удаленной перерегистрацией Интернет-банка потерпевшего, злоумышленники до окончания преступления (т. е. вплоть до перевода денежных средств с вкладов и счетов потерпевшего) находятся с ним на связи. В ряде способов они прямо сообщают потерпевшему о намерении перевода денег с его БПК, он это осознает, но по разным причинам продолжает доверять преступникам. В связи с тем, что обман в указанных случаях направлен непосредственно на завладение чужим имуществом, полагаем, что действия преступников по-прежнему будут образовывать состав мошенничества (в соответствии с ч. 3 п. 2).

[2] Данные номера доступны для приобретения не только юридическим, но и физическим лицам // URL: https://an-telecom.ru/tarifyi (дата обращения: 20.01.2020).

официальную страницу сервиса удаленной регистрации Интернет-банка[1] и вводят туда номер БПК потерпевшего. Владельцу БПК на привязанный к ней телефон приходит цифровой пятизначный СМС-пароль, который преступники под разными предлогами выуживают у потерпевшего с помощью приемов социальной инженерии и в течение двух минут осуществляют перерегистрацию Интернет-банка потерпевшего, установив новый логин и пароль.

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

Для хищения средств со счетов и вкладов также применяются методы социальной инженерии и сначала «для отвода глаз» преступники зачисляют деньги на БПК самого потерпевшего. Это делается для того, чтобы потерпевший поверил в якобы произошедший системный сбой и следовал инструкциям лжеоператоров банка, а кроме того, такая схема позволяет обойти систему фрод-мониторинга банка, делая компьютер злоумышленников доверенным в системе дистанционного банковского обслуживания[2].

Потом преступники перезванивают потерпевшему и под предлогом произошедшего банковского системного сбоя просят вернуть поступившие клиенту деньги назад в банк, передав «оператору» приходящие на телефон пароли. Если им это удается, то денежные средства потерпевшего незамедлительно переводятся на подконтрольные преступникам БПК, банковские счета и балансы мобильных телефонных номеров.

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

- подключают Мобильный банк на телефон мошенников;
- сообщают им реквизиты других своих банковских платежных карт;
- сообщают им логины и пароли от Интернет-банка;
- сами отправляют со своего телефона СМС-оферты для подтверждения операций.

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

---

[1] URL: https://online.sberbank.ru/CSAFront/async/page/registration.do ; URL: https://www.youtube.-com/watch?v=Opa7rXsArqM (дата обращения: 20.01.2020).

[2] Дистанционное банковское обслуживание (ДБО) – общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленно, без непосредственного визита в банк, с использованием компьютерных и телефонных сетей (Клиент-Банк, Интернет-Банк, Мобильный банк и т. д.).

2. Схема телефонных хищений денежных средств физических лиц под видом возникших проблем с законом у их родственника

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

Далее преступник под видом запуганного родственника, изменив голос, (например, произнося слова полушепотом, с хрипотцой или с нотками страха) или незнакомого сотрудника правоохранительного органа, сообщает потерпевшему, что у него самого (если представляется родственником) или у его родственника (если представляется сотрудником) возникли проблемы с законом (он устроил дорожно-транспортное происшествие, сбил человека, задержан с наркотиками, находился за рулем в нетрезвом виде и т. д.), однако еще есть возможность их уладить, заплатив определенную денежную сумму.

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

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

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

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

Подельник преступника, осуществивший снятие денежных средств с банковского счета или с БПК, используя банкомат, терминал самообслуживания, Интернет-банк, осуществляет перевод денежных средств (всех или их часть) преступнику или его родственникам[1].

---

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

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

Преступники связываются с пожилым человеком, пенсионером, обманутым дольщиком, льготником или иным лицом из числа незащищенных слоев населения, позвонив ему на стационарный городской домашний (мобильный) телефон и представляются:

– сотрудниками Пенсионного фонда Российской Федерации (ПФР);

– сотрудниками Банка;

– сотрудниками службы социальной защиты населения;

– сотрудниками ОВД, прокуратуры, или иных правоохранительных органов.

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

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

– он не пользуется социальными пособиями и ему полагается компенсация;

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

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

– из открытых источников в сети «Интернет»;

– используя утечку из правоохранительных органов;

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

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

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

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

– сообщает свои персональные данные;

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

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

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

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

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

– интернет-хищения безналичных денежных средств физических лиц на российских торговых интернет-площадках бесплатных объявлений;

– интернет-хищения безналичных денежных средств физических лиц в интернет-магазинах;

– интернет-хищения безналичных денежных средств физических лиц в социальных сетях и Skype.

Рассмотрим подробно каждый из перечисленных способов:

Схема интернет-хищений безналичных денежных средств физических лиц на российских торговых интернет-площадках бесплатных объявлений:

Первый вариант – «преступник–покупатель»:

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

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

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

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

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

Второй вариант – «преступник-продавец»:

Преступники сами размещают объявление на подходящей торговой интернет-площадке (о сдаче жилья, продаже машины, квартиры, антиквариата или любого другого предмета), указывают телефон и (или) адрес электронной почты для обратной связи и ждут потенциального добросовестного покупателя (клиента). Характерной особенностью привлечения потенциальных клиентов является указание в объявлении самой низкой рыночной цены, обещание бесплатной доставки и другие неоспоримые преимущества, создающие впечатление максимальной выгоды.

Когда поступает звонок от лица, готового приобрести товар, ему предлагается внести предоплату или полную сумму переводом на банковский счет, БПК, электронный кошелек, или на счет телефонного номера.

Показывать товар злоумышленники под разными предлогами отказываются и предлагают переслать фотографию товара на электронную почту.

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

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

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

Бывали случаи, когда несмотря на внесенную предоплату, преступники под различными предлогами просили перевести еще денег. Например, в назначенный день встречи (передачи товара, услуги) сообщали, что не смогут приехать, так как им не выплатили зарплату, их машина сломалась и нужны деньги на такси, на ремонт машины и прочее. Примечательно, что преступники, промышляющие этим способом, не гнушаются даже небольших сумм от 1 до 5 тыс. руб., что является лишним подтверждением участия в этом лиц, находящихся в местах лишения свободы или недавно освободившихся, не имеющих постоянного источника дохода.

Схема интернет-хищений безналичных денежных средств физических лиц в интернет-магазинах:

Преступники создают в Интернете сайт под видом интернет-магазина, в котором предлагают клиентам различный ассортимент популярных товаров. Особенностью привлечения потенциальных клиентов является указание самой низкой рыночной цены, обещание бесплатной доставки и другие неоспоримые преимущества, создающие впечатление максимальной выгоды.

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

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

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

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

Некоторое время после перечисления потерпевшим денежных средств, с целью сокрытия следов своей преступной деятельности злоумышленники отвечают потерпевшему на его звонки и электронные письма, убеждают клиента в выполнении своих обязательств, объясняя задержку доставки товара различными непредвиденными обстоятельствами (задержками на таможне, проблемами у поставщика, большим количеством заказов, блокировкой банковских счетов, ожиданием поставки указанной покупателем комплектации и т. д.).

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

Схема интернет-хищений безналичных денежных средств физических лиц в социальных сетях и Skype:

Первый вариант – «от имени друга»:

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

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

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

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

входа в «Сбербанк Онлайн», после чего похищают средства со счетов и вкладов потерпевшего.

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

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

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

Второй вариант – «от имени сотрудника банка».

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

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

---

[1] Фишинг (англ. phishing, от fishing «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям // URL: https://ru.wikipedia.org/wiki/Фишинг (дата обращения: 25.01.2020).

[2] Хакинг – внесение изменений в программном обеспечении, для достижения определенных целей, отличающихся от целей создателей программ, очень часто изменения являются вредоносными / Что такое хакинг и как от него обезопасить свой компьютер? // URL: http://procomputer.su/comp-gramotnost/164-chto-takoe-khaking-i-kak-obezopasit-kompyuter (дата обращения: 25.01.2020).

ЗАКЛЮЧЕНИЕ

Сегодня практически никто не ставит под сомнение тот факт, что в ближайшем будущем компьютеризация различных сфер общественных отношений лишь увеличится. Это в свою очередь породит не только положительные последствия, но и комплекс социальных проблем и криминальных угроз. Следует обратить внимание, что статистика последних трех лет демонстрирует увеличение количества зарегистрированных преступлений в сфере информационных технологий более чем на 300 %, при этом раскрываемость подобных преступлений приравнивается к 20 %. Какими бы ни были негативные последствия информатизации, очевидно, что никто и никогда не откажется от интернет-банкинга, высокотехнологичной медицины, социальных сетей, многопользовательских онлайн-игр и т. д.

Данный вид преступлений является самым латентным, так как лица, сталкивающиеся с получением фишинговых писем, взломом своих социальных сетей, попыткой хищения электронных денежных средств или средств с банковского счета, не всегда обращаются с заявлением в соответствующие органы. В связи с этим общество столкнулось с необходимостью решения двух задач: построения эффективной системы защиты информации и информационной инфраструктуры, а также приведения в соответствие сложившихся положений законодательства с последствиями глобальной информатизации преступности.

Несмотря на масштаб и сложность проблемы эффективного противодействия преступлениям, совершаемым с использованием информационных технологий, предполагается, что модернизация закона должна осуществляться крайне осторожно, по принципу минимизации вносимых поправок. Нет никакой необходимости сплошного насыщения уголовно-правовых норм указанием на возможность совершения преступления с использованием информационных технологий. Такие оговорки должны иметь место только в случаях очевидных пробелов в уголовном кодексе и его очевидного несоответствия современным угрозам. Взаимосвязь современных программно-аппаратных комплексов, технических навыков и знаний в области права позволит успешно противодействовать новым вызовам и угрозам преступников.

Неотложной и значимой задачей является формирование единообразной правоприменительной практики в условиях имеющегося нормативного материала, что, как представляется, потребует не только определенного времени, но и научных наработок, готовых к противодействию новым способам информационной преступности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Основная литература

1. Stefano Mele. Legal consideration on cyber-weapons and their definition // Journal of Law & Cyber Warfare. – 2014. – Volume 3, Issue 1.

2. Административная деятельность полиции : учебник / под ред. Ю. Н. Демидова. – М. : Юнити-Дана : Закон и право, 2014.

3. Административное право России / под ред. В. Я. Кикотя [и др.]. – 5-е изд., перераб. и доп. – М. : ЮНИТИ-ДАТА, 2012. – 759 с.

4. Административное право : учебник / под ред. Л. Л. Попова, М. С. Студеникиной. – М. : Норма : ИНФРА-М, 2016. – 704 с.

5. Алексеев, С. С. Механизм правового регулирования в социалистическом государстве / С. С. Алексеев. – М. : Юридическая литература, 1966. – 187 с.

6. Арзамасцев, М. В. К вопросу об уголовно-правовой классификации киберпреступлений / М. В. Арзамасцева // Актуальные вопросы права и отраслевых наук. – 2017. – № 1 (3). – С. 11–17.

7. Бергер, Д. Фрод с применением методов социальной инженерии / Д. Бергер [и др.]. – Новосибирск, 2018.

8. Будаковский, Д. С. Способы совершения преступлений в сфере компьютерной информации / Д. С. Будаковский // Российский следователь. – 2011. – № 4. – С. 22.

9. Букалерова, Л. А. О необходимости усиления правовой охраны оборота электронной подписи: современные проблемы теории и практики / Л. А. Букалерова, Р. В. Шагиева // Ученые труды Российской академии адвокатуры и нотариата. – 2011. – № 2 (21). – С. 119–124.

10. Вехов, В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления / В. Б. Вехов // Расследование преступлений: проблемы и пути их решения. – 2015. – № 2 (8). – С. 45.

11. Гилинский, Я. И. Криминологические основы уголовного права в эпоху постмодерна // Криминологические основы уголовного права : материалы X Российского конгресса уголовного права, состоявшегося 26–27 мая 2016 г. / Я. И. Гилинский ; отв. ред. В. С. Комиссаров. – М., 2016. – С. 296.

12. Голуб, В. А., Проблема корректного определения термина «вредоносная программа» / В. А. Голуб, М. В. Овчинникова // Вестник Воронежского государственного университета.

13. Гостева, М. Б. Преступления в сфере компьютерной информации: проблемы и недостатки новой редакции / М. Б. Гостева // Проблемы права. – 2012. – № 5. – С. 121.

14. Гузеева, О. С. Квалификация преступлений в сфере компьютерной информации / О. С. Гузеева. – М., 2016. – С 30.

15. Гузеева, О. С. Преступления, совершаемые в российском сегменте сети «Интернет» : монография / О. С. Гузеева. – М. : Академия Генеральной прокуратуры Российской Федерации, 2015. – С. 37.

16. Доронин, А. М. Уголовная ответственность за неправомерный доступ к компьютерной информации : автореф. дис. … канд. юрид. наук. – М., 2003. – С. 6.

17. Дуленко, В. А. Преступления в сфере высоких технологий / В. А. Дуленко. – М. : ЦОКР МВД России, 2010.

18. Евдокимов, К. Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : монография / К. Н. Евдокимов. – Иркутск, 2013. – С. 60.

19. Ефремова, М. А. Электронный документ как предмет преступления / М. А. Ефремова // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2015. – № 5. – С. 10–15.

20. Зуйков, Г. Г. Поиск преступников по признакам способов совершения преступлений : учебное пособие / Г. Г. Зуйков. – М. : ВШ МВД СССР, 1970. – С. 4.

21. Иванов, И. С. Современный подход к определению мер уголовной ответственности за хищение денежных средств, находящихся на банковском счете, и электронных денежных средств / И. С. Иванов, С. В. Рязанцева // Российский следователь. – 2018. – № 8. – С. 49.

22. Иванова, Е. В. Официальный документ в электронной форме как предмет преступления, предусмотренного ст. 327 УК РФ / Е. В. Иванова // Уголовное право. – 2012. – № 3. – С. 29–31.

23. Казарин, О. В. Вредоносные программы нового поколения – одна из существующих угроз международной информационной безопасности / О. В. Казарин, Р. А. Шаряпов // Вестник РГГУ. – Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2015. – № 12 (155). – С. 9–23.

24. Кибальник, А. Г. Квалификация мошенничества в новом постановлении Пленума Верховного Суда Российской Федерации / А. Г. Кибальник // Уголовное право. – 2018. – № 1. – С. 61.

25. Козаев, Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства) : монография / Н. Ш. Козаев. – М. : Юрлитинформ, 2015. – С. 172.

26. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа // дисс. … канд. юрид. наук. – Иркутск, 2017. – С. 88.

27. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) // под ред. С. В. Дьякова, Н. Г. Кадникова. – 5-е изд., перераб. и доп. – М. : Юриспруденция, 2017.

28. Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

29. Лебедева, А. А. Актуальные вопросы квалификации мошенничества в сфере компьютерной информации / А. А. Лебедева // Безопасность бизнеса. – 2018. – № 5.

30. Лопашенко, Н. А. Уголовно-правовая и криминологическая политика государства в области высоких технологий / Н. А. Лопашенко // URL: http://sartraccc.ru/i.-php?filename=Pub%2Flopashenko%2830-06%29.htm&oper=read_file (дата обращения: 10.01.2020).

31. Лукьянова, А. А. Электронный официальный документ как предмет преступления, предусмотренного ст. 327 УК РФ / А. А. Лукьянова // Уголовное право. – 2016. – № 3. – С. 57–62.

32. Малышенко, Д. Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. … канд. юрид. наук. – М., 2002. – С. 58.

33. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

34. Руденков, Н. А. Основы сетевых технологий : учебник для вузов / Н. А. Руденков, Л. И. Долинер. – Екатеринбург : Уральский Федеральный университет, 2011. – 300 с.

35. Пикуров, Н. И. Квалификация преступлений с бланкетными признаками состава : монография / Н. И. Пикуров. – М., 2009. – С. 138.

36. Поветкина, Н. А. Правовая форма интеграции информационных систем и информационных технологий в сферу публичных финансов / Н. А. Поветкина // Журнал российского права. – 2018. – № 5. – С. 96–112.

37. Шурухнов, Н. Г. Расследование неправомерного доступа к компьютерной информации : учебное пособие / Н. Г. Шурухнов [и др.]. – 2-е изд., перераб. и доп. – М. : Московский университет МВД России, 2004. – С. 173.

38. Решетников А. Ю. Квалификация неоконченных преступлений при наличии признаков совокупности преступлений / А. Ю. Решетников // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2016. – № 4. – С. 85.

39. Романова, А. С. Борьба с преступностью в компьютерных сетях «глубинного интернета» / Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования : материалы Всероссийской научно-практической конференции (29 апреля 2016 г.) / А. С. Романова ; под ред. П. А. Капустюк, Р. А. Забавко. – Иркутск : ФГКОУ ВО ВСИ МВД России, 2016. – 152 с.

40. Российской уголовное право. Общая часть : учебник / под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. – 2 изд., перераб. и доп. – М., 2010. – С. 42.

41. Русскевич, Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учебное пособие / Е. А. Русскевич. – М. : Научно-издательский центр ИНФРА-М, 2017. – 115 с.

42. Савенков, А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности / А. Н. Савенков // Государство и право. – 2017. – № 10. – С. 5–18.

43. Степанов, А. Н. Информатика для студентов гуманитарных специальностей : учебник для вузов / А. Н. Степанов. – 3-е изд. – СПб. : Питер, 2002. – 608 с.

44. Тер-Акопов, А. А. Преступление и проблемы нефизической причинности в уголовном праве : монография / А. А. Тер-Акопов. – М. : Юркнига, 2003. – 480 с.

45. Тюнин, В. И. Мошенничество в сфере компьютерной информации: сложности квалификации / В. И. Тюнин // Уголовное право. – 2017. – № 5. – С. 95.

46. Уголовное право. Особенная часть : учебник / под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева – М., ИНФРА-М, 2008. – 800 с.

47. Фатьянов, А. А. Правовое обеспечение безопасности информации в Российской Федерации : учебное пособие / А. А. Фатьянов. – М., 2001. – С. 40.

48. Фролов, А. А. Исследование механизмов рассмотрения, запрещенного содержимого в DARKNET / А. А. Фролов, Д. С. Сильнов // Современные информационные технологии и ИТ-образование. – 2017. – № 4. – С. 216–224.

49. Хабриева, Т. Я. Право в условиях цифровой реальности / Т. Я. Хабриева, Н. Н.Черногор // Журнал российского права. – 2018. – № 1. – С. 85–102.

50. Халиуллин, А. И. Вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации / А. И. Халиулин // Труды Академии управления МВД России. – 2011. – № 4. – С. 88.

51. Хилюта, В. В. Вопросы квалификации преступлений против собственности, не являющихся хищением : монография / В. В. Хилюта. – Минск, 2013. – С. 33.

52. Хисамова, З. И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий : анализ изменений законодательства и правоприменительной практики / З. И. Хисамова // Российский следователь. – 2018. – № 9. – С. 46.

53. Худяков, П. В. Расследование преступлений в сфере компьютерной информации : учебно-методическое пособие / П. В. Худяков. – М. : ДГСК МВД России, 2011. – 128 с.

54. Чупрова, А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий / А. Ю. Чупрова // Уголовное право. – 2015. – № 5. – С. 133.

55. Чупрова, А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции : дис. … д-ра юрид. наук. – М., 2015. – С. 48.

56. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – М. : ДМК Пресс, 2014. – 702 с.

57. Швед, Н. А. Неправомерный доступ к компьютерной информации: уголовно-правовая защита в Российской Федерации и Республике Беларусь / Н. А. Швед // Информационное право. – 2016. – № 2. – С. 32.

58. Ягудин, А. Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей : автореф. … дис. канд. юрид. наук. – М., 2013. – С. 14.

Нормативные правовые акты

1. Конституция Российской Федерации от 12 декабря 1993 г. (в действующей редакции) // Собрание законодательства Российской Федерации. – 2009. – № 4, ст. 445.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 1996. – № 25, ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2001. – № 52 (ч. 1), ст. 4921.

4. Гражданский кодекс Российской Федерации. Часть первая от 30 ноября 1994 г. № 51-ФЗ (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 1994. – № 32, ст. 3301.

5. Гражданский кодекс Российской Федерации. Часть вторая от 26 января 1996 г. № 14-ФЗ (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 1996. – № 5, ст. 410.

6. Гражданский кодекс Российской Федерации. Часть третья от 26 ноября 2001 г. № 146-ФЗ (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2001. – № 49, ст. 4552.

7. Гражданский кодекс Российской Федерации. Часть четвертая от 18 декабря 2006 г. № 230-ФЗ (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2006. – № 52 (1 ч.), ст. 5496.

8. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2002. – № 1 (ч. 1), ст. 1.

9. Федеральный закон Российской Федерации от 7 февраля 2011 г. № 3-ФЗ «О полиции» (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2011. – № 7, ст. 900.

10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с последующими изменениями и дополнениями) // Российская газета. – 2006. – № 165 (29 июля).

11. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» (с послед. изм. и доп.) // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. 1), ст. 3451.

12. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2001. – № 23, ст. 2291.

13. Федеральный закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

14. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 1995. – № 33, ст. 3349.

15. Указ Президента Российской Федерации от 15 января 2013 г. № 31 с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства Российской Федерации. – 2013. – № 3, ст. 178.

16. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

17. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

18. Приказ МВД России № 1144 от 3 декабря 2007 г. «О системе информационного обеспечения Госавтоинспекции» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

19. Приказ МВД России от 29 августа 2014 г. № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

20. Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст).

21. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

22. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

Материалы правоприменительной практики

1. Апелляционный приговор Судебной коллегии по уголовным делам Верховного суда Чувашской Республики от 3 июня 2015 г. по делу № 22-1054/2015.

2. Всестороннее исследование проблемы киберпреступности // Управление Организации Объединенных Наций по наркотикам и преступности / Vienna International Centre, PO Box 500, 1400 Vienna, Austria.

3. Дело о фишинге: как ловили хакеров-близнецов из Санкт-Петербурга // URL: https://ria.ru/incidents/ 20121221/915789715.html (дата обращения: 10.01.2020).

4. Братья по кибероружию. Хакеры-близнецы Дмитрий и Евгений Попелыши сели в тюрьму со второго раза // URL: https://www/group-ib.ru/blog/brothers (дата обращения: 10.01.2020).

5. Постановление Пленума Верховного суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

6. Информационно-аналитические материалы Следственного департамента МВД России за 2015 г.

7. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

8. Обвинительное заключение по уголовному делу № 100995 // Архив СУ МУ МВД России «Коломенское».

9. Обвинительное заключение по уголовному делу № 1146014 // Архив СЧ СУ МВД по Республике Адыгея.

10. Обвинительное заключение по уголовному делу № 423731 // Архив СО Корякского МО МВД России // Задержаны хакеры, взламывавшие по заказам страницы в соцсетях, почтовые ящики и занимавшиеся «прослушкой» // URL: https://мвд.рф-news/show_102385 (дата обращения: 26.08.2019).

11. Обзор судебной практики Верховного Суда Российской Федерации № 3, 2017 (утв. Президиумом Верховного Суда Российской Федерации 12 июля 2017 г.) //

СПС «КонсультантПлюс». – URL: http://www.consultant.ru (дата обращения: 10.01.2020).

12. Приговор Александровского городского суда Владимирской области от 19 августа 2015 г. по делу № 1-82/2015.

13. Приговор Ново-Савинского районного суда г. Казани от 16 ноября 2018 г. по делу № 1-525/2018.

14. Приговор Октябрьского районного суда г. Архангельска от 14 декабря 2015 г. по делу № 1-352/2015.

15. Приговор Октябрьского районного суда г. Ижевска от 23 июня 2014 г. по делу № 1-186/14.

16. Приговор Первомайского районного суда Оренбургской области от 8 июля 2016 г. по делу № 1-58/2016.

17. Приговор Первомайского суда г. Кирова от 9 сентября 2016 г. по делу № 1-222/2016.

18. Приговор Пресненского районного суда г. Москвы от 23 января 2014 г. по делу № 1-43/2014.

19. Приговор Смольнинского районного суда г. Санкт-Петербург от 2 февраля 2011 г. по делу № 1-65/11.

20. Приговор Советского районного суда г. Орска Оренбургской области от 17 августа 2018 г. по делу № 1-240/2018.

21. Приговор Советского районного суда г. Улан-Удэ Республика Бурятия от 22 сентября 2015 г. по делу № 1-715/2015.

22. Приговор Солнцевского районного суда г. Москвы от 6 ноября 2018 г. по делу № 1-318/18.

23. Приговор Бийского городского суда от 26 марта 2015 г. по делу № 1-250/2015.

24. Приговор Центрального районного суда г. Воронежа от 25 октября 2018 г. по делу № 1-312/2018.

25. Приговор Богдановичского городского суда Свердловской области от 27 августа 2015 г. по делу № 1-30/2015.

26. Приговор Катайского районного суда Курганской области от 18 апреля 2013 г. по делу № 1-20/2013.

27. Приговор Кировградского городского суда Свердловской области от 5 августа 2016 г. по делу № 1-105/2016.

28. Приговор Курганского городского суда от 21 сентября 2015 г. по делу № 1-1388/15.

29. Приговор Ленинского районного суда г. Смоленска от 20 сентября 2018 г. по делу № 1-275/2018.

30. Приговор Муромского городского суда Владимирской области от 30 ноября 2018 г. по делу № 1-297/2018.

31. Приговор Салаватского городского суда Республики Башкортостан от 21 мая 2015 г. по делу № 1-113/2015 Хамовнического районного суда г. Москвы от 15 мая 2014 г. по делу № 1-49/2014.

32. Постановление Лефортовского районного суда г. Москвы от 13 января 2015 г. по делу № 1-401/2014 (дело было прекращено по основаниям, предусмотренным ст. 78 УК РФ).

33. Постановление о прекращении уголовного дела Лефортовского районного суда г. Москвы от 13 января 2015 г. по делу № 1-401/2014.

34. Приговор Домодедовского городского суда Московской области от 6 ноября 2018 г. по делу № 1-399/2018.

35. Постановление Президиума Верховного Суда Российской Федерации от 25 декабря 1996 г. № 436п96 по делу В. П. Ткаченко и В. В. Хоперского // Бюллетень Верховного Суда Российской Федерации. – 1997. – № 4.

36. Постановление Президиума Верховного Суда Российской Федерации от 20 августа 2003 г. № 495п03 по делу С. И. Бычкало и др. // Бюллетень Верховного Суда Российской Федерации. – 2004. – № 3.

37. Решение коллегии Министерства внутренних дел Российской Федерации России от 1 ноября 2019 г. № 3 км.

Электронные ресурсы

1. The Global Risks Report 2016 // URL: http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/world-economic-forum-global-risk-report-2016.pdf (дата обращения: 27.06.2019).

2. Владимир Путин назвал спецслужбы США источником вируса WannaCry. – URL: http://www.kommersant.ru/doc/3297338 (дата обращения: 20.11.2019).

3. URL: https://online.sberbank.ru/CSAFront/async/page/registration.do.

4. URL: https://www.youtube.com/watch?v=Opa7rXsArqM.

5. Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике / С. Н. Потапкин [и др.]. – URL: https://base.garant.ru/57488207/.

6. Ложная тревога // URL: https://rg.ru/2017/09/12/reg-pfo/v-krupnyh-gorodah-rossii-evakuirovali-desiatki-shkol-vokzalov-i-tc.html (дата обращения: 15.04.2019).

7. Российские компании потеряли не менее 116 млрд руб. от кибератак в 2017 г. // URL : https://www.nafi.ru/analytics/rossiyskie-kompanii-poteryali-ne-menee-116-mlrd-rubley-ot-kiberatak-v-2017-godu/ (дата обращения: 30.06.2019).

8. Телефонные террористы дозвонились в Москву // URL: https://www.kommersant.ru/doc/3409928 (дата обращения: 15.05.2019).

9. Уголовный кодекс Азербайджанской Республики от 30 декабря 1999 г. № 787-IQ (с изм. и доп. по сост. на 31.05.2016) // URL : http://online.zakon.kz/m/Document/?docid=30420353#sub_id=2710000 (дата обращения: 07.11.2019).

10. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. №226-V (с изм. и доп. по сост. на 11.07.2017) // URL : http://online.zakon.kz/m/Document/?doc_id=33-885902 #sub_id=320200 (дата обращения: 07.11.2019).

ПРИЛОЖЕНИЯ

Приложение 1

УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
ОБЩИЕ ПОЛОЖЕНИЯ

Учебная дисциплина «Расследование преступлений в сфере компьютерной информации» является важной профилирующей дисциплиной, обеспечивающей профессиональное обучение слушателей Московского университета МВД России имени В.Я. Кикотя.

Целью данной учебной дисциплины является формирование у слушателей профессиональных знаний и выработка необходимых навыков по применению положений уголовного и уголовно-процессуального законодательства, рекомендаций науки и правоприменительной практики при расследовании преступлений в сфере компьютерной информации.

Основными задачами учебной дисциплины являются:

– ознакомление слушателей с основными нормативными правовыми актами, регламентирующими правоотношения в сфере компьютерной информации;

– ознакомление слушателей с рекомендациями уголовно–процессуальной и криминалистической науки, правоприменительной практики по вопросам организации расследования преступлений указанной категории;

– обучение слушателей комплексному применению имеющихся у них теоретических знаний в условиях решения организационно-правовых проблем, характерных для процесса расследования преступлений в сфере компьютерной информации;

– формирование у слушателей практических навыков необходимых для успешного расследования преступлений в сфере компьютерной информации.

В результате изучения дисциплины «Расследование преступлений в сфере компьютерной информации» слушатели должны:

– знать законы и подзаконные акты, применяемые в процессе расследования преступлений указанной категории;

– уметь комплексно применять имеющиеся теоретические знания и практические навыки в наиболее типичных ситуациях, характерных для процесса расследования преступлений в сфере компьютерной информации;

– иметь навыки составления наиболее сложных процессуальных документов (постановления о возбуждении уголовного дела, постановления о назначении судебных экспертиз, постановления о привлечении лица в качестве обвиняемого и др.).

На изучение учебной дисциплины «Расследование преступлений, в сфере компьютерной информации» по очной форме обучения отводится 60 ч, из них 40 ч – аудиторные занятия, 20 ч – самостоятельная работа.

В лекционном материале по данной учебной дисциплине предлагаются основные прикладные положения методики расследования преступлений в сфере компьютерной информации, рассматриваются соответствующие положения действующего законодательства, теоретические проблемы и спорные вопросы расследования преступлений в сфере компьютерной информации (в том числе в финансово-кредитной сфере), которые требуют разрешения.

Основное внимание в процессе обучения отводится практическим занятиям, формированию у слушателей профессиональных навыков и практических умений, необходимых следователю при расследовании преступлений данной категории.

В процессе обучения слушатели выполняют практикум, который оформляется в виде учебного уголовного дела. Успешное выполнение заданий по данному практикуму является обязательным условием допуска к зачету.

Формой итогового контроля по результатам обучения является зачет.

Тематика занятий по дисциплине «Расследование преступлений в сфере компьютерной информации» для слушателей очной формы обучения

№ темы	Название темы	Всего	В том числе					Примечание
			Лекции	Семинары	Практические занятия	Деловые игры	Контрольные работы	
1	Правовые основы и особенности расследования отдельных видов преступлений в сфере компьютерной информации	6	2	–	4	–		
2	Планирование и организация деятельности следователя на этапе возбуждения уголовного дела	8	–	–	8	–		
3	Планирование, организация и производство процессуальных и следственных действий на начальном этапе расследования	16	2	–	8	6		
4	Планирование и организация деятельности следователя на последующем и заключительном этапах расследования	10		–	10			
	Практикум							
	ВСЕГО:	**40**	**4**	**–**	**30**	**6**		
	Зачет							

Последовательность прохождения учебных занятий:

Л. 1-2; п. 1 (4) – входное тестирование; п. 2.1 (4); п. 2.2 (4); Л.3-4; п. 3.1 (4); п. 3.2 (4); Д/И.3.3 (6) – деловая игра на криминалистическом полигоне; П. 4.1.1 – выходное тестирование, П. 4.1.2 – встреча с практиком; П. 4.2 (6) – выезд на Коптево.

Ф А Б У Л А
УЧЕБНОГО УГОЛОВНОГО ДЕЛА

11 февраля текущего года в отдел «К» ГУ МВД России по г. Москва поступила информация о том, что в различных отделах полиции г. Москвы увеличилось количество регистрируемых обращений граждан, клиентов ПАО «Банк Восход» и других банков о несанкционированных операциях по банковским картам, а именно о снятии денежных средств в январе текущего года. В ходе анализа поступившей информации было установлено, что несанкционированные снятия денежных средств имеют общие места осуществления банковских операций – дополнительный офис № 7-77 ПАО «Банк Восход», расположенный по адресу: г. Москва, ул. Окружной проезд д. 44 а.

В ходе проведенной проверки были затребованы копии видеозаписей с банкоматов и средств видео-регистрации в указанном офисе. При их просмотре были выделены изображения нескольких лиц, которые совершали действия несвойственные для лиц, желающих воспользоваться банкоматом. Также при просмотре видеозаписи было видно, что указанные лица постоянно пользовались сотовым телефоном.

Идентифицировать личности граждан, зафиксированных на видеозаписях, не представилось возможным, поскольку лица были закрыты головными уборами. Однако, были установлены номера телефонов, которыми пользовались правонарушители в момент совершения хищений и установки скиммингового оборудования.

В ходе дальнейшей проверки по установленному номеру телефона из социальной сети «В контакте» было получено изображение П. П. Петрова, которое по некоторым признакам совпало с изображением лица, зафиксированного камерами внутри дополнительного офиса № 7-77 ПАО «Банк Восход».

Так же было установлено, что во время снятия денежных средств П. П. Петров постоянно связывался по телефону со своим знакомым Б. Б. Громовым.

В дальнейшем была получена информация, что П. П. Петров и Б. Б. Громов готовятся снять, ранее установленное скимминговое оборудование на одном из банкоматов ПАО «Банк Восход».

19 февраля текущего года по адресу: г. Москва, ул. Большая Черкизовская, д. 12 П. П. Петров был задержан сотрудниками отдела «К» ГУ МВД России по г. Москва, при демонтаже скимминговго оборудования из банкомата. В его сумке был обнаружен еще один комплект скимминговго оборудования (накладка на банкомат с видеокамерой и устройства для записи информации на магнитные полосы карт), деньги, белые карты.

Б. Б. Громов при попытке задержания, скрылся на своей автомашине.

С П Р А В К А по учебному уголовному делу

1. Преступление выявлено 11 февраля текущего года.

2. Уголовное дело возбуждено следователем 19 февраля текущего года.

3. 19 февраля текущего года П. П. Петров был задержан.

4. Петров Петр Петрович, 1995 г. р. студент Московского политехнического университета. Проживает с родителями В. П. Петровым и Т. М. Петровой по адресу: г. Москва, просп. Волгина, д. 33, кв. 11.

5. 20 февраля текущего года П. П. Петрову избрана мера пресечения – заключение под стражу.

6. При допросе подозреваемый П. П. Петров сообщил, что монтаж и демонтаж установленных технических средств на банкоматы ПАО «Банк Восход» он производил со своим знакомым Б. Б. Громовым с целью получения данных для изготовления дубликатов карт клиентов банкомата, пользовавшихся его услугами, и дальнейшего хищения денежных средств с их счетов. Однако реализовать до конца преступный умысел, направленный на хищение денежных средств граждан не смогли по независящим от их воли обстоятельствам, поскольку сотрудники полиции его задержали в момент демонтажа специальных технических средств, предназначенных для негласного получения информации с вышеуказанного банкомата.

7. Согласно заключению эксперта № 74/777, изъятое в ходе задержания у гражданина Петрова устройство для считывания информации с банковских карт, камера видеозаписи относятся к категории специальных технических средств, предназначенных для негласного получения информации.

8. Р. Ю. Котов – свидетель, заместитель начальника отдела «К» БСТМ ГУ МВД Росси по г. Москва, который сообщил, что в январе- феврале текущего года отделом проводилось документирование и пресечение преступной деятельности лиц, осуществляющих скимминг. В январе в их поле зрения попали П. П. Петров и Б. Б. Громов, когда сотрудники отдела стали просматривать записи с камер видеонаблюдения, в районе установки скимминговогo оборудования и установили нескольких лиц. Затем отделом проводилось ОРМ «Наблюдение» в отношении Петрова П. П. и Громова Б. Б., получены сведения о их преступной деятельности на территории г. Москва. В ходе проведенных мероприятий был задержан П. П. Петров при попытке снятия скимминговогo оборудования в отделении ПАО «Банк Восход». После этого он проводил личный досмотр П. П. Петрова, в ходе которого изъял деньги, белые пластиковые карты, на которых были наклеены липкие ленты с 4 цифрами на каждой и комплект скимминговогo оборудования. Петров П. П. пояснил Котову Р. Ю., что карты принадлежат ему. Также рядом с ним были изъяты солнцезащитные очки и головной убор. Было установлено, что по дороге к дополнительному офису ПАО «Банк Восход», расположенному по адресу: г. Москва, ул. Большая Черкизовская, д 12, П. П. Петров и Б. Б. Громов переодевались в специально подготовленную верхнюю одежду. При задержании П. П. Петрова рядом находилась автомашина Lexus LX-570, госномер Е777ЕН 77, водитель которой скрылся при появлении сотрудников полиции. Как выяснилось позже данной машиной управлял Б. Б. Громов.

Свидетель Р. Ю. Котов так же пояснил, что 27 февраля он участвовал в обыске по месту жительства Б. Б. Громова, где были изъяты белые пластиковые карты, устройство для записи информации на магнитную полосу, электронные носители информации.

9. 27 февраля по месту жительства Б. Б. Громова по адресу: г. Москва, ул. Большая Тульская, д. 10/15, кв. 75 был произведен обыск, в ходе которого задержан сам Громов Б. Б., а также было обнаружено и изъято техническое средство, которое согласно заключению эксперта № 76/777, относится к категории специальных технических средств, предназначенных для негласного получения аудио-видеоинформации. Кроме того, были изъяты оптический диск «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов» и несъемный магнитный жесткий диск (НМЖД) «Samsung» 500 GB с надписью: «Софт для копирования карт», устройство для записи информации на магнитные полосы карт, «белый пластик» для заготовки чистых карт в количестве 50 шт.

10. Громов Б. Б. сообщил, что три комплекта скиммингового оборудования, программное обеспечение и комплект оборудования для изготовления копий банковский карт он в период времени с февраля по май прошлого года, приобрел посредством сети «Интернет» и браузера «Tor», обеспечивающего анонимность работы в сети. Два скимминговых комплекта он передал своему знакомому П. П. Петрову, а остальное оборудование хранил дома до момента изъятия сотрудниками полиции при обыске.

11. А. А. Зайцев – юрист ПАО «Банк Восход» – представитель потерпевшего, сообщил, что в результате преступных действий П. П. Петрова и Б. Б. Громова вкладчикам – клиентам ПАО «Банк Восход» материальный ущерб причинен не был, так как банк возместил им похищенные средства в размере 2 159 550 руб.

12. В. В. Андреев – свидетель, начальник службы экономической безопасности ПАО «Банк Восход», пояснил что по факту нескольких обращений клиентов о несогласии с банковскими операциями, при которых с их банковских карт произошло несанкционированное снятие денежных средств, сотрудники банка провели внутреннее разбирательство, в результате которого было установлено, что произошла компрометация нескольких банковских карт, принадлежащих клиентам ПАО «Банк Восход».

Также В. В. Андреев пояснил, что при просмотре сотрудниками банка сохранившиеся видеозаписей с камер скрытого видео-наблюдения, установленного в банкомате и помещении, где он находится, было выявлено, что в дни компрометации карт появляются одни и те же молодые люди – парни 20–30 лет. При этом они вели себя подозрительно, ни как клиенты, желающие воспользоваться банкоматом. Каждый из них в разные дни выполняет определенные действия: крепит что-то к стене над банкоматом и выполняет те или иные операции с банкоматом. При этом сотрудники банка предполагают, что персональные данные клиентов были считаны при помощи скимминг–устройства, устанавливаемого на банкомат для негласного получения «пин-кода» и данных магнитной полосы банковской карты.

Кроме того, В. В. Андреев обратил внимание на дату несанкционированных снятий денежных средств, а именно 16 ноября прошлого года с 00 ч 17 мин до 00 ч 19 мин по адресу: г. Москва, ул. Окружной проезд, д. 44 а, посредством банкомата № 00182039, принадлежащим ПАО «Банк Восход».

Дополнительно В. В. Андреев сообщил, что банковские карты их клиентов имеют микропроцессор, а банкомат ПАО «Банк Восход», откуда были сняты деньги, не предназначен был обрабатывать микропроцессорные карты, и провел операцию только по магнитной полосе. В указанном случае произошел неправомерный доступ к охраняемой законом компьютерной информации, принадлежащей ПАО «Банк Восход», который повлек копирование компьютерной информации и собирание сведений, составляющих банковскую тайну незаконным способом, на что распространяют свое действие:

– ч. 4 ст. 10 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», в соответствии с которой предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией;

– ст. 26 Федерального закона Российской Федерации от 2 декабря 1990 г. № 395-1-ФЗ «О банках и банковской деятельности», в соответствии с которой информация о денежных средствах, содержащихся на банковских счетах законных держате-

лей банковских карт, их персональных данных и идентификационных номерах-кодах, является сведениями, составляющими коммерческую и банковскую тайну;

– ч. 1 ст. 1225 Гражданского кодекса Российской Федерации, в соответствии с которой программы для ЭВМ и базы данных являются результатами интеллектуальной деятельности, которым предоставляется правовая охрана;

– ч. 2 ст. 1260 Гражданского кодекса Российской Федерации, в соответствии с которой базой данных является предоставленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы материалы могли быть найдены и обработаны с помощью ЭВМ.

13. При осмотре оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов» обнаружена программа для сопряжения портативного считывателя магнитных полос, которые специально разработаны для сбора данных с магнитной полосы, с файлами для работы данной программы, в которых имеются шифрованные и дешифрованные данные считанные с магнитных полос карт, видео файлами, программной частью, необходимой для сопряжения устройства чтения/записи карт с магнитной полосой «MSR606», программной частью – инструментом, который позволяет просматривать содержимое Chip& PIN/EMV.

14. В результате проведенной компьютерно-технической экспертизы НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», изъятых при обыске в квартире Громова Б. Б., обнаружена информация, представляющая интерес для следствия. А именно: наличие программного продукта «MagCard Write/Read Utility Program v2.01», расположенного в «раздел № 2: / Program Files (×86) / MSR606/», папка создана 30 июля 2016 г. В окне загруженного программного продукта обнаружена надпись «Magnetic Stripe Card Reader / Writer»[1]. При подключенном устройстве для чтения / записи с пластиковых карт с магнитной полосой «MSR206u» и загруженном программном продукте, в качестве экспертного эксперимента, были проведены операции чтение, копирование и запись. Исходя из полученных результатов сделан вывод о том, что при помощи данного продукта возможно проводить считывание магнитных полос банковских карт и записывать их на «белый пластик».

[1] Magnetic Stripe Card Reader / Writer – перевод с английского Магнитная полоса карты считывание / записывание.

Практикум (учебное уголовное дело) должен содержать в себе следующие документы:

1. Титульный лист.
2. Опись документов.
3. План первоначальных проверочных действий.
4. Протокол осмотра места происшествия – места установки банкомата в дополнительном офисе № 7-77 ПАО «Банк Восход», расположенном по адресу: г. Москва, ул. Окружной проезд, д. 44 а.
5. Постановление о возбуждении уголовного дела и принятии его к производству.
6. Протокол допроса свидетеля В. В. Андреева.
7. Протокол допроса свидетеля Р. Ю. Котова.
8. Протокол допроса представителя потерпевшего А. А. Зайцева.
9. Протокол задержания П. П. Петрова.
10. Протокол допроса подозреваемого П. П. Петрова.
11. Ходатайство в суд об избрании П. П. Петрову меры пресечения в виде заключения под стражу.
12. Поручение о производстве оперативно-разыскных мероприятий направленных на установление каналов поступления и мест возможного сбыта специальных технических средств, предназначенных для негласного получения информации и вредоносных программ, предназначенных для копирования информации с магнитных полос банковских карт.
13. Постановление о назначении компьютерно-технической экспертизы НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт» и оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов».
14. Постановление следователя о производстве обыска в квартире Б. Б. Громова.
15. Протокол обыска в квартире Б. Б. Громова по адресу: г. Москва, ул. Большая Тульская, д. 10/15, кв. 75 (на основании ч. 5 ст. 165 и ст. 182 УПК РФ).
16. Протокол осмотра НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов», комплекта скиммингового оборудования.
17. Постановление о признании и приобщении к уголовному делу в качестве вещественных доказательств – НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов», комплекта скиммингового оборудования.
18. Постановление о привлечении П. П. Петрова в качестве обвиняемого.
19. Обвинительное заключение.

При недостаточности сведений из фабулы учебного уголовного дела и справки (число, дата, Ф.И.О. и т. д.) слушатель самостоятельно моделирует недостающую информацию и вносит ее в текст составляемых документов.

Тема 1. Правовые основы и особенности расследования отдельных видов преступлений в сфере компьютерной информации

Практическое занятие № 1: 1–4 часа

Проводится входное тестирование

Цель занятия: систематизация ранее полученных знаний и формирование новых умений необходимых для расследования преступлений в сфере компьютерной информации; получение и освоение новых знаний по теме занятия.

Вопросы для рассмотрения

1. Действующее законодательство Российской Федерации, регулирующее правоотношения в сфере компьютерной информации.
2. Основные понятия, применяемые в гл. 28 УК РФ.
3. Общая уголовно-правовая характеристика преступлений, предусмотренных ст.ст. 272–274 УК РФ.
4. Криминалистическая характеристика преступлений в сфере компьютерной информации.

Методические рекомендации

При ответе на первый вопрос следует указать основные нормативно-правовые акты и их положения регламентирующие правоотношения в сфере компьютерной информации.

При ответе на второй вопрос следует раскрыть содержание таких понятий как: охраняемая законом компьютерная информация, неправомерный доступ к компьютерной информации, уничтожение информации, блокирование информации, модификация информации, копирование тяжкие последствия, существенный вред и некоторых других, использующихся в гл. 28 УК РФ.

При ответе на третий и четвертый вопросы следует раскрыть сущность основных элементов уголовно-правовой и криминалистической характеристики преступлений в сфере компьютерной информации.

Решение задач по теме № 1

Практическая ситуация № 1

В период с 1 августа по 11 ноября прошлого года С. А. Салов, находясь в своей квартире по адресу: г. Москва, просп. Славы, д. 22, кв. 11, используя персональный компьютер, самодельный программатор сим-карт, а также программы ЭВМ, позволяющие несанкционированно копировать, модифицировать и уничтожать компьютерную информацию, находящуюся на сим-карте оператора сотовой связи, осуществил несанкционированное копирование информации, находящейся на сим-картах ряда абонентов операторов сотовой связи ОАО «МТМ».

Согласно перечню сведений, составляющих коммерческую тайну, ОАО «МТМ», информация о сим-картах с содержащейся на них информацией отнесена к коммерческой тайне.

1. Содержатся ли в действиях С. А. Салова признаки преступления.

Если да, то какого именно?

2. По какому признаку информация на сим-картах относится к компьютерной.

Практическая ситуация № 2

Р. Ю. Котов в период с апреля по август прошлого года в городе Москве посредством персонального компьютера, Wi-Fi-модема EMI 23455431 из своей квартиры, расположенной по адресу: г. Москва, просп. Волина, д. 12 кв. 4, незаконно подключился к роутеру гражданина С. А. Ноева и скопировал логин, пароль работы в сети «Интернет», предоставленный на основании договора поставщиком интернет-услуг С. А. Ноеву. В дальнейшем Котов неоднократно под этим логином и паролем работал в сети «Интернет». При этом доступ в сеть С. А. Ноева при подключении к сети «Интернет» Р. Ю. Котова блокировался.

1. Содержатся ли в действиях Р. Ю. Котова признаки преступления?

Если да, то какого именно?

2. Определите место происшествия исходя из обстоятельств, предлагаемых в фабуле.

3. Кто, с учетом указанных обстоятельств, может быть признан потерпевшим?

Практическая ситуация № 3

В период с января по март текущего года неустановленные лица осуществляли неправомерный доступ к охраняемой законом компьютерной информации – ключам аутентификации «Ki» и электронным номерам «IMSI», находящимся на сим-картах сотовых телефонов стандарта GSM, зарегистрированных в сети филиала сотовой связи ОАО «Район77», при незаконном изготовлении копий сим-карт. Указанный неправомерный доступ повлек копирование данной информации с оригинальной сим-карты на заготовку копии. Были установлены лица, совершившие указанное преступление.

1. Составьте перечень проверочных действий по данному факту.

2. Квалифицируйте действия лиц, совершивших преступление, с учетом обстоятельств, указанных в фабуле.

Практическая ситуация № 4

В период с февраля по март текущего года Т. А.Тайзинов, находясь в доме, расположенном по адресу: г. Белгород, ул. Б. Хмельницкого, д. 56, работая с ЭВМ в сети «Интернет», с неустановленного следствием сайта перенес установочный пакет программы «Сниффер», являющейся анализатором сетевого трафика и позволяющей без уведомления собственника собирать информацию о принадлежащих этим собственникам логинах и паролях, а также копировать данную информацию на жесткий диск своего компьютера. Зная о вредоносных функциях указанной программы, Т. А. Тайзинов скопировал ее на флеш-карту своего знакомого К. А. Перова по его просьбе.

Содержатся ли в действиях Тайзинова Т. А. признаки преступления.

Если да, то какого именно?

Практическая ситуация № 5

25 января текущего года в 10:30 оперативными сотрудниками отдела «К» БСТМ ГУ МВД России по Московской области была проведена проверочная закупка 10 оптических компакт-дисков с программами для ЭВМ в торговом павильоне фирмы ООО «Гигабит». В ходе предварительного исследования компьютерной информации, содержащейся на компакт-дисках, на трех из них были обнаружены вредоносные программы для ЭВМ.

Содержатся ли в действиях продавца и владельца ООО «Гигабит» признаки преступления? Если да, то какого именно?

Практическая ситуация № 6

А. Ю. Сазонов изготовил компьютерную программу «25к», использующую принцип 25-го кадра и оказывающую скрытое воздействие на подсознание пользователей с целью активизации у последних намерений покупать рекламируемые товары. О данной программе он сообщил своему знакомому А. Е. Фиронову, который сообщил о программе «25к» в ОВД.

Содержатся ли в действиях А. Ю. Сазонова признаки преступления? Если да, то какого именно?

Практическая ситуация № 7

При плановой проверке радиорынков столицы был задержан гражданин А. И. Суренков, который распространял на радиорынке «Савелов двор» компакт диски с информацией об общественном объединении «Формат России». Данная организация включена в опубликованный перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности».

Содержатся ли в действиях А. И. Суренкова признаки преступления?
Если да, то какого именно?

Самостоятельная работа по теме № 1

1. Повторить рассмотренный на занятии материал.
2. Изучить предлагаемую дополнительную литературу и правовые акты.
3. Подготовиться к теоретическим вопросам и практическим заданиям следующей темы.

Дополнительная литература к теме № 1

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2004. – № 32, ст. 3283.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2006. – № 31 (1 ч.), ст. 3448.

Федеральный закон от 1 октября 2008 г. № 164-ФЗ «О ратификации Соглашения о сотрудничестве государств–участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» // Собрание законодательства Российской Федерации. – 2008. – № 40, ст. 4499.

Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении правил оказания услуг связи по передаче данных» (с последующими изм. и доп.) // Собрание законодательства Российской Федерации. – 2006. – № 5, ст. 553.

Постановление Правительства Российской Федерации от 28 апреля 2006 г. № 252 «О лицензировании деятельности по изготовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин (программ для

ЭВМ), баз данных и фонограмм на любых видах носителей (за исключением случаев, если указанная деятельность самостоятельно осуществляется лицами, обладающими правами на использование указанных объектов авторских и смежных прав в силу федерального закона или договора» (с последующими изменениями и дополнениями) // Собрание законодательства Российской Федерации. – 2006. – № 19, ст. 2078.

Государственный стандарт ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

Национальный стандарт ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

Вехов, В. Б. Уголовная ответственность за сетевые вирусные атаки / В. Б. Вехов // Защита информации. Инсайд. – 2005. – № 3. – С. 21.

Использование современных технологий и проблемы информационной безопасности в деятельности правоохранительных органов // Сборник научных статей. – Калининград : филиал СпбУ МВД России, 2012.

Смушкин, А. Б. Виртуальные следы в криминалистике / А. Б. Смушкин // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

Ткачев, А. В. Исследование компьютерной информации в криминалистике / А. В. Ткачев // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

Тема 2. Планирование и организация деятельности следователя на этапе возбуждения уголовного дела

Практические занятия – 8 часов

Практическое занятие № 2.1: 4 часа

Цель занятия: уяснение правовых и теоретических вопросов порядка приема, регистрации и проверки заявлений о преступлении в сфере компьютерной информации.

Вопросы для рассмотрения

1. Поводы и основание к возбуждению уголовного дела о преступлении в сфере компьютерной информации.

2. Особенности возбуждения уголовного дела о преступлении в сфере компьютерной информации.

Методические рекомендации

Отвечая на первый вопрос, слушатели должны знать не только положения гл. 19 УПК РФ, но и ведомственные правовые акты, регламентирующие деятельность ОВД при приеме и регистрации заявлений о преступлении. Изложить порядок регистрации сообщений о преступлении в ОВД.

Отвечая на второй вопрос, необходимо обратить внимание, что при возбуждении уголовных дел в сфере компьютерной информации, нередко используются результаты ОРД. Необходимо проанализировать нормы, регламентирующие использование результатов оперативно-разыскной деятельности (ст. 11 ФЗ об ОРД, ст. 89 УПК РФ).

Решение задач к практическому занятию № 2.1

Практическая ситуация № 1

11 января текущего года в дежурную часть ОМВД по району «Нагатинский» г. Москвы обратился гражданин А. В. Ивашов с устным заявлением следующего содержания:

«В 2015 г. я заключил договор № 1234 о предоставлении мне услуг по доступу к информационным ресурсам сети «Интернет» с ООО «4 Ком». При заключении договора я получил индивидуальное имя пользователя (логин) WW1978 и пароль, который никому не сообщал. Соединение с сетью «Интернет» я всегда осуществлял с использованием принадлежащих мне персональной ЭВМ и WI-FI роутера «ASUS» с\н A4568BN74. С 29 августа по 29 сентября этого же года я находился в летнем ежегодном отпуске в республике Индонезия. Вернувшись из отпуска, я с удивлением обнаружил в своем почтовом ящике извещение на оплату услуг «Интернет» на мое имя за август и сентябрь текущего года на сумму 5 000 руб. 5 октября я обратился к представителям ООО «4 Ком» за разъяснениями по данному вопросу, которые передали мне статистику обращения в сеть «Интернет» под моим логином за август месяц. Ознакомившись с содержанием распечатки информации, полученной из учетной базы данных ООО «4 Ком» об оказанных услугах по доступу к сети «Интернет», я увидел, что под моим логином в сеть «Интернет» входили и работали неизвестные мне лица, причиненный ущерб в размере 5 000 руб. является для меня значительным».

Для составления протокола принятия устного заявления о преступлении в сфере компьютерной информации гражданин А. В. Ивашов был направлен оперативным дежурным в кабинет № 216 к дежурному следователю.

Придя в назначенное помещение, по просьбе следователя, заявитель предъявил паспорт серии 77 02 № 546 789, выданный 7 мая 2001 г. Центральным ОВД г. Курска на имя Ивашова Андрея Владимировича, русского, родившегося 13 февраля 1978 г. в г. Москве, зарегистрированного по адресу: Московская область г. Можайск, ул. Советская, д. 2, кв. 1.

1. Проанализируйте предлагаемую ситуацию.

2. Составьте протокол принятия устного заявления у А. В. Ивашова.

3. Составьте план проверки сообщения о преступлении, указав в нем неотложные следственные действия и оперативно-разыскные мероприятия, которые необходимо выполнить по закреплению следов преступления и установлению правонарушителя.

Практическая ситуация № 2

5 мая текущего года сотрудниками отдела «К» БСТМ ГУ МВД России по г. Москве, в рамках проведения операции «Сеть-2015» и отработки оперативной информации об организованной группе лиц, занимающихся разработкой и распространением вредоносных программ для ЭВМ, на территории одного из торгово-выставочных центров произведен комплекс оперативно-разыскных мероприятий.

При осуществлении сбыта компакт-дисков, содержащих вредоносные программы для ЭВМ (компьютерные вирусы, программы для взлома компьютерных сетей), задержан гражданин С. А. Колосов. У него обнаружены машинные носители информации, содержащие 765 вредоносных программ.

1. Определите, какой документ будет являться поводом для возбуждения уголовного дела в указанной ситуации.

2. Определите комплекс действий по проверке этого сообщения.

Практическая ситуация № 3

Неизвестные лица, в период с 1 мая 2010 г. по 12 июня 2009 г., находясь по адресу: г. Москва, ул. Шариковая 2–11 и располагая информацией относительно заключенного договора № 131/УД от 01 сентября 2005 г. и кодами доступа к электронной программе «модуль платежей», осуществили неправомерный доступ к охраняемой законом компьютерной информации – к сведениям об обеспечении информационно-технологического взаимодействия между ОАО «Кибер-Ком» и коммерческим банком «Юнайт», содержащимся на сервере ОАО «Кибер-Ком» по адресу: г. Москва, Краснопресненская набережная, 140, что повлекло копирование и модификацию информации.

1. Содержатся ли в действиях указанных лиц признаки преступления?

Если да, то какого именно?

2. С учетом предлагаемых обстоятельств определите место происшествия.

Задание к практическому занятию № 2.1

Проанализируйте фабулу учебного уголовного дела и справку по учебному уголовному делу (стр. 7–10).

Квалифицируйте действия П. П. Петрова и Б. Б. Громова.

Составьте план первоначальных проверочных действий.

Практическое занятие № 2.2: 2–4 часа

Цель занятия: уяснение слушателями особенностей производства процессуальных действий на этапе возбуждения уголовного дела, специфики взаимодействия следователя с иными подразделениями органов внутренних дел, выработка способности слушателей комплексно использовать теоретические и правовые знания при составлении процессуальных документов.

Вопросы для рассмотрения

1. Процессуальные действия следователя на этапе возбуждения уголовного дела о преступлении в сфере компьютерной информации.

2. Виды и формы взаимодействия, осуществляемого следователем с подразделениями ОВД в ходе расследования преступления в сфере компьютерной информации.

Методические рекомендации

Отвечая на 1-й вопрос следует перечислить действия, направленные на установление оснований, достаточных для возбуждения уголовного дела.

Отвечая на 2-й вопрос необходимо назвать подразделения ОВД, с которыми следователь взаимодействует при расследовании преступлений в сфере компьютерной информации. Указать формы такого взаимодействия. Особое внимание следует уделить взаимодействию следователя с подразделениями «К» МВД России.

Решение задач к практическому занятию № 2.2

Практическая ситуация № 1

8 мая текущего года в ГУ МВД РФ по г. Москве поступило заявление В. К. Карпенко, заместителя директора ООО «МАСКА», о том, что абонент ООО «МАСКА» И. В. Баринов, который в соответствии с договором абонентского обслуживания № 3 587 имел доступ в сеть «Интернет» и электронный почтовый ящик на почтовом сервере ООО «МАСКА», открыл на сервере ООО «МАСКА» персональную страницу, на которую в апреле текущего года скопировал программу regedit.exe.

Проведенной специалистами ООО «МАСКА» проверкой было установлено, что в структуре файла regedit.exe содержится вредоносная программа, с помощью которой можно получить несанкционированный доступ к компьютерной информации других пользователей сети «Интернет».

1. Есть ли основания для принятия решения о возбуждении уголовного дела?

2. Составьте перечень проверочных действий по данному факту.

3. Составьте постановление о возбуждении уголовного дела.

4. Составьте план первоначальных организационных и следственных действий.

Практическая ситуация № 2

В период с сентября 2015 г. по февраль текущего года неизвестный, используя персональный компьютер, подключенный к локальной компьютерной сети ООО «ТОРИ», осуществлял неправомерный доступ к охраняемой законом компьютерной информации, находящейся на машинном носителе, установленном по адресу: г. Москва, ул. Победы, д. 21 в сети организации-провайдера ООО «ТОРИ». Незаконные подключения к сети «Интернет» осуществлялись под логином и паролем, предоставленным согласно договору № 14 от 12 января 2014 г. клиенту ООО «ТОРИ» – О. С. Сомову.

1. Содержатся ли в действиях указанного лица признаки преступления.
Если да, то какого именно?
2. Составьте перечень первоначальных процессуальных действий.

Практическая ситуация № 3

А. А. Исаев разместил в локальной сети своего района несколько вредоносных программ, с помощью которых пользователям удавалось обходить защитные модули лицензионных программ. В ходе проведения операции «Сеть-2015» А. А. Исаев был задержан сотрудниками отдела «К».

По данному факту возбуждено уголовное дело.

1. Квалифицируйте деяние.

2. Составьте перечень первоначальных организационных и процессуальных действий следователя.

3. Решите вопрос о необходимости избрания в отношении А. А. Исаева меры пресечения.

Задание к практическому занятию № 2.2

Проанализируйте фабулу учебного уголовного дела и составьте следующие процессуальные документы:

– протокол осмотра места происшествия – места установки банкомата в дополнительном офисе № 7–77 ПАО «Банк Восход», расположенном по адресу: г. Москва, ул. Окружной проезд, д. 44 а;

– постановление о возбуждении уголовного дела и принятии его к производству.

Самостоятельная работа по теме № 2

1. Повторите рассмотренный на занятиях материал, при необходимости оформите процессуальные документы.

2. Изучить предлагаемую дополнительную литературу.

3. Подготовиться к правовым вопросам и практическим заданиям следующей темы.

Практическая ситуация № 1 см[1]

11 февраля текущего года в период с 12 ч до 13 ч К. Е. Сомов, находясь по адресу: г. Москва, ул. Карла Маркса, д. 2, реализуя нелицензионные экземпляры программных продуктов, установил на машинный носитель ЭВМ, находящийся в данном офисе, нелицензионный экземпляр программного продукта «1С: Предприятие 8.0 для SQL Комплексная поставка», правообладателем которого является ЗАО «1С» (г. Москва), кроме того, запустил вредоносную программу – «патчер» (эмулятор ключа) – «Sable» (Сэйбл), предназначенную для взлома системы защиты программного продукта путем неправомерного доступа к защищаемой законом компьютерной информации.

При установке нелицензионного программного продукта «1С: Предприятие 8.0 для SQL Комплексная поставка», с целью нейтрализации средств защиты программного продукта, К. Е. Сомов использовал вредоносную компьютерную программу – эмулятор ключа, которая приводит к несанкционированному блокированию информации, передаваемой аппаратным ключом защиты, и модификации программного продукта «1С: Предприятие 7.7 для SQL Комплексная поставка» в части изменения средств индивидуальной защиты.

[1] Здесь и далее знак «см» указывает на задание, отнесенное к самостоятельной работе учащихся.

После чего машинный носитель с указанным нелицензионным продуктом К. Е. Сомов предложил купить С. А. Кротову за 2 000 руб., однако С. А. Кротов обратился с заявлением в отдел «К» БСТМ ГУ МВД России по г. Москве.

1. Что будет являться в указанной ситуации поводом для возбуждения уголовного дела?

2. Определите алгоритм действий по проверке данного заявления.

Практическая ситуация № 2 см

В период с 4 по 5 мая текущего года неизвестное лицо осуществило неправомерный доступ к охраняемой законом компьютерной информации – имени пользователя и паролю электронного почтового ящика гражданина А. А. Сараева.

По данному факту возбуждено уголовное дело.

1. По описанной фабуле определите форму и порядок взаимодействия следователя с органом дознания.

2. По описанной фабуле укажите перечень процессуальных и следственных действий, где следователю требуется участие сотрудников органа дознания.

Практическая ситуация № 3 см

18 января текущего года в период с 10 ч 45 мин до 15 ч в ходе проведения ОРМ сотрудниками отдела «К» БСТМ, был задержан гражданин А. А. Ситник, который, находясь в офисе Сервис-центра, действуя на основании заключенного договора возмездного оказания услуг, за вознаграждение в размере 3 000 руб., незаконно, без разрешения правообладателя, вмонтировал в электронную схему игровой компьютерной приставки «SONY PlayStation-3» (Сони Плейстейшн-3) с серийным номером D 212345 элементный модуль (чип), в котором заложена программа для ЭВМ, позволяющая блокировать программу защиты, модифицировать внутреннее программное обеспечение и нарушать нормальный режим работы компьютерной приставки.

1. Укажите порядок предоставления результатов ОРМ следователю.

2. Определите форму и порядок взаимодействия следователя с органом дознания в указанной ситуации.

Дополнительная литература по теме № 2

Ищенко, П. П. Информационное обеспечение следственной деятельности : научно-практическое пособие / П. П. Ищенко. – М. : Юрлитинформ, 2011.

Погодин, И. В. Преступления экстремистской направленности : методика доказывания : монография / И. В. Погодин. – М. : Юрлитинформ, 2012.

Родин, А. Ф. Расследование преступлений в сфере компьютерной информации : учебно-методическое пособие / А. Ф. Родин. – М. : ЦОКР МВД России, 2008.

Тема 3. Планирование, организация и производство процессуальных и следственных действий на начальном этапе расследования

Практические занятия – 14 часов

Практическое занятие № 3.1: 4 часа

Цель занятия: систематизация ранее полученных правовых и теоретических знаний, формирование новых умений необходимых для осуществления процессуальных действий на начальном этапе расследования преступлений в сфере компьютерной информации.

Вопросы для рассмотрения

1. Организация и тактические особенности подготовки и производства допроса потерпевших от совершения преступлений в сфере компьютерной информации.
2. Организация и тактические особенности подготовки и производства допроса подозреваемых в совершении преступлений в сфере компьютерной информации.
3. Особенности задержания и избрания меры пресечения при расследовании преступлений в сфере компьютерной информации.
4. Деятельность следователя по подготовке к назначению компьютерно-технических экспертиз.

Методические рекомендации

При подготовке к ответу на первый и второй вопросы следует помнить, что допрос – это следственное действие, заключающееся в получении и фиксации в установленном законом порядке показаний участников уголовного судопроизводства. Необходимо повторить положения гл. 26 УПК РФ, регламентирующие основания и процессуальный порядок производства допроса, ст.ст. 187–191 УПК РФ. Следует помнить, что процессуальный порядок, организационные и тактические особенности подготовки и производства допроса различаются в зависимости от процессуального положения допрашиваемого его возраста, состава участников следственного действия, характера следственной ситуации и других обстоятельств дела.

При подготовке к ответу на третий вопрос необходимо помнить, что лица совершающие преступления в сфере компьютерной информации, не редко обладают глубокими техническими познаниями, активно используют электронные носители информации, содержащие важную для расследования информацию, соответственно при их задержании целесообразно привлекать специалиста соответствующего профиля.

При рассмотрении особенностей избрания меры пресечения, следует учесть тот факт, что лица, совершающие преступления в сфере компьютерной информации, с использованием браузера, обеспечивающего анонимность работы в информационно-телекоммуникационной сети «Интернет» – TOR, имеют возможность заказать фальшивые документы, удостоверяющие личность, организовать анонимное давление на потерпевших и свидетелей. При ответе необходимо обратиться к нормам, содержащимся в гл. 13 УПК РФ. Особое внимание следует уделить основаниям избрания, изменения и отмены меры пресечения.

Задание к практическому занятию № 3.1

В соответствии с фабулой учебного уголовного дела, составьте следующие процессуальные документы:

1. Протокол допроса свидетеля В. В. Андреева.
2. Протокол допроса свидетеля Р. Ю. Котова.
3. Протокол допроса представителя потерпевшего А. А. Зайцева.
4. Протокол задержания П. П. Петрова.
5. Протокол допроса подозреваемого П. П. Петрова.
6. Ходатайство в суд об избрании П. П. Петрову меры пресечения в виде заключения под стражу.

Практическое занятие № 3.2: – 4 часа

Цель занятия: получение и усвоение новых, а также систематизация ранее полученных правовых и теоретических знаний об особенностях участия в расследовании преступлений рассматриваемой категории специалистов и назначении типичных экспертиз.

Вопросы для рассмотрения

1. Виды наиболее типичных экспертиз, назначаемых по делам о преступлениях в сфере компьютерной информации.
2. Типичные вопросы, подлежащие разрешению в ходе судебных компьютерно-технических экспертиз.
3. Процессуальный порядок работы следователя с вещественными доказательствами – электронными носителями информации.
4. Участие эксперта и специалиста в расследовании преступлений в сфере компьютерной информации.

Методические рекомендации

При ответе на первый вопрос необходимо пояснить какие экспертизы целесообразно назначать при расследовании данной категории преступлений. Рассматривая основания и процессуальный порядок назначения и проведения судебных экспертиз, необходимо ознакомиться с гл. 27 УПК РФ, а также знать особенности процессуального статуса специалиста и эксперта, как участников уголовного судопроизводства (ст.ст. 57 и 58 УПК РФ).

При ответе на второй вопрос следует, исходя из разновидностей компьютерно-технических экспертиз, указать наиболее типичные вопросы, которые подлежат разрешению экспертом.

При ответе на вопрос о вещественных доказательствах, необходимо знать, что вещественными являются доказательства, сформированные путем отражения информации на материальных объектах. Перечень предметов, признаваемых вещественными доказательствами, указан в ст. 81 УПК РФ, порядок хранения вещественных доказательств в ст. 82 УПК России. Особое внимание необходимо уделить особенностям работы с электронными носителями информации, как вещественными доказательствами.

При ответе на четвертый вопрос необходимо знать, что является предметом показаний специалиста и эксперта. Рассмотреть ситуации и следственные действия, при которых следователю целесообразно привлечь специалиста. Указать цель и значение его участия, в производстве по делу.

Рассматривая участие эксперта и специалиста в уголовном судопроизводстве, необходимо повторить положения ст.ст. 57 и 58 УПК РФ.

Решение задач к практическому занятию № 3.2

Практическая ситуация № 1

12 января текущего года в 11 часов у входа на станцию метро «Павелецкая» г. Москвы при продаже проездных билетов на электропоезда сотрудниками ППС был задержан 19-летний студент одного из вузов – А. К. Андров. При досмотре в его рюкзаке оказалось 545 билетов на 1 поездку в метро, имеющих одинаковую серию и номер. Билеты были в виде бумажной карты с узкой магнитной полосой. Для выяснения обстоятельств А. К. Андров был доставлен в ОМВД.

1. Определите вид необходимой компьютерно-технической экспертизы по данному факту.

2. Составьте перечень вопросов к эксперту по данному факту.

Практическая ситуация № 2

17 апреля текущего года на Царицынском радиорынке г. Москвы при проведении проверочной закупки у предпринимателя без образования юридического лица гражданина М. Н. Петрова были обнаружены и изъяты оптические компакт-диски следующего содержания:

– базы данных Главного управления по обеспечению безопасности дорожного движения МВД России с идентификационными данными владельцев и угнанных у них автомототранспортных средств – 101 экземпляр;

– базы данных московских операторов электросвязи МГТС, МСС и Билайн GSM с персональными данными обслуживаемых абонентов – 67 экземпляров.

1. Определите вид необходимой компьютерно-технической экспертизы по данному факту.

2. Составьте перечень вопросов к эксперту по данному факту.

Практическая ситуация № 3

При установке нелицензионного программного продукта «1С: Бухгалтерия» Д. В. Зыкин, с целью нейтрализации средств защиты программного продукта, использовал вредоносную компьютерную программу – эмулятор ключа, которая приводит к несанкционированному блокированию информации, передаваемой аппаратным ключом защиты, и модификации программного продукта «1С: Предприятие 7.7 для SQL Комплексная поставка» в части изменения средств индивидуальной защиты.

По данному факту возбуждено уголовное дело.

1. Какие виды экспертиз необходимо назначить в указанной ситуации.

Составьте вопросы эксперту.

2. Определите, какие объекты необходимо предоставить на экспертизу.

Задание к практическому занятию № 3.2

В соответствии с фабулой учебного уголовного дела, составьте следующие процессуальные документы:

1. Поручение о производстве оперативно-разыскных мероприятий направленных на установление каналов поступления и мест возможного сбыта специальных технических средств, предназначенных для негласного получения информации и вредоносных программ, предназначенных для копирования информации с магнитных полос банковских карт.

2. Постановление о назначении компьютерно-технической экспертизы НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт» и оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов».

Практическое занятие № 3.3 – 6 часов

Занятие проводится в компьютерном классе и на полигоне

В компьютерном классе возможен просмотр учебного фильма, слайдов, характеризующих особенности расследования преступлений в сфере компьютерной информации, рассматриваются теоретические вопросы, занятия – 2 часа. На криминалистическом полигоне занятие проводится в форме деловой игры – 4 часа.

Цель занятия: усвоение новых и повторение основных правовых и теоретических положений, регулирующих основания и процессуальный порядок производства обыска и различных видов осмотров, уяснение особенностей осмотра электронных носителей информации.

Вопросы для рассмотрения

1. Основания и процессуальный порядок производства осмотра предметов и документов.

2. Подготовка и планирование производства осмотра предметов и документов при расследовании преступлений в сфере компьютерной информации.

3. Порядок процессуального оформления хода и результатов осмотра предметов и документов при расследовании преступлений в сфере компьютерной информации.

4. Организация и осуществление обыска при расследовании преступлений в сфере компьютерной информации

Методические рекомендации

При ответе на вопросы данного занятия и при теоретической подготовке к проведению ролевых игр, необходимо повторить положения ст.ст. 166, 167, 176, 177, 180, 182 УПК РФ, соответствующие положения криминалистической тактики производства обысков и осмотров предметов, а также методики расследования данной группы преступлений.

На практическом занятии проводятся две ролевых игры:

– обыск в квартире Б. Б. Громова – (ролевая игра № 1);

– осмотр электронных носителей информации – НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов», комплекта скиммингового оборудования (ролевая игра № 2).

Ролевая игра № 1 проводится в несколько этапов:

1. Этап – подготовительный. Перед началом проведения ролевой игры «Обыск в жилище» преподаватель прорабатывает с обучаемыми тактические особенности подготовки и проведения данного следственного действия. Акцентируется внимание обучаемых на необходимость и важность предварительного изучения характеристик помещения, в котором планируется осуществить обыск, а также данных характеризующих проживающих в нем лиц.

На данном этапе необходимо обратить особое внимание обучаемых на положения ч. 9.1 ст. 182 УПК РФ, которые регламентируют особенности работы с электронными носителями информации при производстве обыска.

Затем преподаватель формирует несколько рабочих групп, в состав которых включает: следователя, специалиста, двух понятых, нескольких сотрудников оперативных подразделений органов внутренних дел и нескольких наблюдателей (лиц, оценивающих ход следственного действия), участникам разъясняются их функциональные обязанности.

2. Этап – рабочий. На нем осуществляется непосредственная работа по обыску в квартире, где проживает Б. Б. Громов – лицо, которое приобрело три комплекта скиммингового оборудования, программное обеспечение и комплект оборудования для изготовления копий банковский карт посредством сети «Интернет» и браузера «Tor», обеспечивающего анонимность работы в сети. Результаты обыска фиксируются в «черновом» варианте соответствующего протокола.

3. Этап – заключительный. На данном этапе подводятся итоги занятия. Преподаватель обращает внимание на положительные стороны проведенного обыска в жилище, указывает на допущенные ошибки. Наиболее отличившимся слушателям выставляются оценки.

Ролевая игра № 2 проводится так же в несколько этапов:

Этап – подготовительный. Преподаватель, отбирает группу наиболее подготовленных слушателей, которые будут выполнять роль следователей и осуществлять осмотр предметов НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов», комплекта скиммингового оборудования, ранее изъятые при обыске в квартире Б. Б. Громова и поступившие следователю после проведения компьютерно-технической экспертизы. Содержание НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», оптического диска «Verbatim» DVD-RW 8x с надписью: «Взломщик кодов»[1].

1. Этап – рабочий. На нем осуществляется непосредственная работа по осмотру НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов», комплекта скиммингового оборудования – одной группой слушателей (следователями) и фиксация его результатов (в черновом варианте) – другой группой слушателей (наблюдателями).

2. Этап – заключительный. На данном этапе подводятся итоги занятия. Преподаватель обращает внимание на положительные стороны проведенного осмотра, указывает на допущенные ошибки. Наиболее отличившимся слушателям выставляются оценки.

Задание к практическому занятию № 3.3

В соответствии с фабулой учебного уголовного дела составьте следующие процессуальные документы:

1. Постановление следователя о производстве обыска в квартире Б. Б. Громова.

[1] Смотреть справку по делу.

2. Протокол обыска в квартире Б. Б. Громова по адресу: г. Москва, ул. Большая Тульская, д. 10/15, кв. 75 (на основании ч. 5 ст. 165 и ст. 182 УПК РФ).

3. Протокол осмотра НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов», комплекта скиммингового оборудования.

4. Постановление о признании и приобщении к уголовному делу в качестве вещественных доказательств – НМЖД «Samsung» 500 GB с надписью: «Софт для копирования карт», оптического диска «Verbatim» DVD-RW 8× с надписью: «Взломщик кодов», комплекта скиммингового оборудования.

Самостоятельная работа по теме № 3

1. Повторить рассмотренный на занятиях материал, при необходимости оформить процессуальные документы.

2. Изучить предлагаемую дополнительную литературу.

3. Подготовиться к правовым вопросам и практическим заданиям следующей темы.

Практическая ситуация № 1 см

А. П. Серых достоверно зная, что игровая компьютерная приставка «SONY PlayStation-3» с серийным номером F 090876 содержит несанкционированно внесенный в ее электронную схему элементный модуль (чип), в котором заложена программа для ЭВМ, позволяющая без уведомления собственника информации блокировать программу защиты, модифицировать внутреннее программное обеспечение и нарушать нормальный режим работы компьютерной приставки, 1 августа 2010 г. продал указанную игровую приставку за 7 500 руб. А. А. Арутюнову, распространив, тем самым, машинный носитель с вредоносной программой.

По данному факту возбуждено уголовное дело.

1. Квалифицируйте деяние.

2. Какие виды экспертиз необходимо назначить в указанной ситуации. Составьте вопросы эксперту.

3. Определите, какие объекты необходимо предоставить эксперту?

Практическая ситуация № 2 см

В период с января по февраль текущего года неустановленные лица осуществляли неправомерный доступ к охраняемой законом компьютерной информации – к ключам аутентификации «Ki» и электронным номерам «IMEI», находящимся на сим-картах сотовых телефонов стандарта GSM, зарегистрированных в сети филиала сотовой связи ОАО «ГОР», при незаконном изготовлении копий сим-карт. Указанный неправомерный доступ повлек копирование данной информации с оригинальной сим-карты на копию. Были установлены лица, совершившие указанное преступление.

По данному факту возбуждено уголовное дело. Следователь, готовясь провести обыск, решает вопрос о привлечении специалиста.

1. Определите форму участия специалиста, а также возможна ли в этом случае иная форма участия специалиста.

2. Какие задачи при производстве обыска должен поставить следователь специалисту?

Дополнительная литература к теме № 3

Егорышева, Е. А. Некоторые вопросы использования специальных знаний при расследовании неправомерного доступа к компьютерной информации / Е. А. Егорышева, А. С. Егорышев // СПС «КонсультантПлюс» – URL: https://www.consultant.ru.

Зайцева, Е. А. Применение специальных познаний в уголовном судопроизводстве / Е. А. Зайцева. – Волгоград, 2005.

Зигура, Н. А. Компьютерная информация как вид доказательств в уголовном процессе России : монография / Н. А. Зигура, А. В. Кудрявцева. – М. : Юрлитинформ, 2011.

Косынкин, А. А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования / А. А. Косынкин // СПС «Гарант». – URL: http://base.consultant.ru.

Кушниренко, С. П. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях : учебное пособие / С. П. Кушниренко, Е. И. Панфилова. – 3-е изд., перераб. и доп. – СПб., 2009.

Усов, А. И. Судебно-экспертное исследование компьютерных средств и систем. Основы методического обеспечения : учебное пособие / А. И. Усов ; под ред. Е. Р. Россинской. – М., 2008.

Тема 4. Планирование и организация деятельности следователя на последующем и заключительном этапах расследования

Практические занятия – 10 часов

Практическое занятие № 4.1.1 – 2 часа

Проводится выходное тестирование

Цель занятия: закрепление сформировавшихся навыков при осуществлении последующего и заключительного этапа расследования преступлений в сфере компьютерной информации с составлением соответствующих процессуальных документов. Оформление практикума и сдача его на проверку преподавателю.

Вопросы для рассмотрения

1. Особенности привлечения в качестве обвиняемого в совершении преступлений, в сфере компьютерной информации.
2. Порядок предъявления обвинения.

Методические рекомендации

Выходное тестирование проводится в компьютерном классе.

При подготовке к занятию необходимо изучить положения гл. 23 УПК РФ, регламентирующие основания и процессуальный порядок привлечения лица в качестве обвиняемого и предъявление обвинения (ст.ст. 171–175 УПК РФ).

При составлении процессуальных документов, помимо изученных норм закона необходимо повторить положения главы 29 УПК России.

Самостоятельная работа по теме № 4.1.1

В соответствии с фабулой учебного уголовного дела, составьте следующие процессуальные документы:

1. Постановление о привлечении П. П. Петрова в качестве обвиняемого.
2. Обвинительное заключение.

После составления обвинительного заключения все процессуальные документы прошиваются как макет уголовного дела и сдаются преподавателю.

Практическое занятие № 4.1.2 – 2 часа

Занятие проводится в форме встречи с практическим работником

Цель занятия: контроль полученных в результате обучения знаний и навыков, получение знаний о современных тенденциях расследования преступлений в сфере компьютерной информации.

Методические рекомендации

После выступления практического работника, обучаемым рекомендуется задавать вопросы по особенностям расследования преступлений в сфере компьютерной информации.

Практическое занятие № 4.2 – 6 часов

Проводится выездное занятие на «Факультет подготовки специалистов в области информационной безопасности»

Цель занятия: получение знаний о современных методах и способах электронного противодействия преступлениям в сфере компьютерной информации, особенностях использования высоких технологий в расследовании данных преступлений, ознакомление с основами компьютерной разведки.

Приложение 2

СЛОВАРЬ
основных специальных терминов и выражений

IMSI (International Mobile Subscriber Identity) – это международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи стандарта GSM, UMTS или CDMA. При регистрации в сети аппарат абонента передает IMSI, по которому происходит его идентификация.

MAC-адрес (от англ. Media Access Control – управление доступом к среде, также Hardware Address) – это уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей. В широковещательных сетях (таких, как сети на основе Ethernet) MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне, которую используют протоколы более высокого (сетевого) уровня.

Абонент – пользователь телематическими услугами связи, с которым заключен возмездный договор об оказании телематических услуг связи с выделением уникального кода идентификации.

Абонентская линия – линия связи, соединяющая пользовательское (оконечное) оборудование с узлом связи сети передачи данных;

Абонентский интерфейс – технико-технологические параметры физических цепей, соединяющих средства связи оператора связи с пользовательским (оконечным) оборудованием, а также формализованный набор правил их взаимодействия;

Абонентский терминал – совокупность технических и программных средств, применяемых абонентом и (или) пользователем при пользовании телематическими услугами связи для передачи, приема и отображения электронных сообщений и (или) формирования, хранения и обработки информации, содержащейся в информационной системе.

Автомат – самодействующее техническое устройство (аппарат, машина, прибор), производящее работу по заданной программе без непосредственного участия человека.

Автоматизированная информационная система (АИС) – система автоматизации информационного процесса деятельности человека, т. е. замены труда человека по созданию, сбору, обработке, хранению, передачи и уничтожению информации работой машины; в отличие от автоматической информационной системы всегда функционирует при участии человека, который является ее главным звеном.

Аторизация – процесс удостоверения прав пользователей на осуществление каких-либо действий над компьютерной информацией, содержащейся в системе или сети ЭВМ.

Алгоритм – набор последовательных предписаний (операций), направленных на решение какой-либо задачи.

Антивирусная программа – программа для ЭВМ, предназначенная для поиска, регистрации и уничтожения вредоносных программ для ЭВМ.

Аппаратное средство электронно-вычислительной техники – механическое, магнитное, электрическое, электромагнитное, электронное, оптическое или магнитооптическое устройство (прибор, блок, схема, деталь, проводник), входящее в состав средства электронно-вычислительной техники.

Аппаратный блок – конструктивно оформленная как единое целое совокупность взаимосвязанных технических устройств, либо совокупность взаимосвязанных элементов или узлов одного устройства, выполняющих определенную функцию.

Атрибуты файла – имя, тип (расширение), дата и время создания.

Аттестованное средство электронно-вычислительной техники – средство электронно-вычислительной техники в отношении которого проведено специальное исследование на предмет отсутствия вредоносных программных и аппаратных средств с выдачей Аттестата соответствия требованиям по безопасности информации.

Аутентификация – процедура проверки подлинности, например, проверка подлинности пользователя путем сравнения введенного им пароля с паролем в базе данных пользователей; подтверждение подлинности электронного письма путем проверки цифровой подписи письма по ключу шифрования отправителя.

База данных – объективная форма представления и организации совокупности данных (например, статей, расчетов), систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ.

Базовая система ввода-вывода информации (BIOS) – специальная программа для ЭВМ, записываемая на интегральную микросхему постоянного запоминающего устройства (ПЗУ). BIOS обеспечивает автоматический запуск ЭВМ после включения электропитания и организует базовый процесс ввода-вывода информации на уровне машинных кодов (машинных языков).

Байт – единица измерения информации; наименьшая адресуемая единица данных или памяти ЭВМ. 1 байт – объем емкости памяти, необходимый для хранения в нем 1 символа.

Блокирование компьютерной информации – физическое воздействие на компьютерную информацию, ее машинный носитель и (или) программно-технические средства ее обработки и защиты, результатом которого явилась временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией.

Винчестер (жесткий диск ЭВМ) – машинный носитель информации. Представляет собой малогабаритный пакет жестких магнитных дисков, герметизированных вместе с головками записи-чтения компьютерной информации. Находится внутри системного блока ЭВМ и является ее внешней постоянной несменяемой памятью.

Виртуальный диск – программное представление (имитация) несуществующего физического жесткого диска в виртуальной операционной системе.

Владелец компьютерной информации, информационной системы, технологии и средства их обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Владелец сертификата ключа электронной цифровой подписи (ЭЦП) – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Вредоносная программа для ЭВМ – программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

Вредоносное программное обеспечение – программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя, либо к ухудшению параметров функционирования абонентского терминала или сети связи.

Вспомогательная программа для ЭВМ – программа для ЭВМ, которая расширяет возможности функционирования операционной системы ЭВМ по отдельным направлениям организации процесса автоматической обработки информации. С ее помощью пользователь получает набор дополнительных инструментов по контролю, мониторингу и управлению компонентами ОС, а также внутренними и внешними устройствами ЭВМ.

Гибкий магнитный диск (ГМД или флоппи-диск) – машинный носитель информации. Является сменным постоянным носителем компьютерной информации. Используется в качестве внешней памяти прямого доступа. Изготовлен в форме диска из полимерного тонкопленочного материала, имеющего специальное ферромагнитное покрытие. Выпускаются диски диаметром 200 мм (8 дюймов), 133 мм (5,25 дюйма) и 90 мм (3,5 дюйма). Диск находится в защитном пластмассовом корпусе квадратной формы.

Данные – формализованное представление сведений, доступное для обработки, интерпретации и обмена между людьми или в автоматическом режиме с использованием СВТ.

Декомпилятор – программа для ЭВМ, выполняющая функцию, обратную *транслятору*: воспроизводит и преобразуют объектный код в исходный текст (с машинного языка на язык программирования). Входит в состав системы программирования.

Дискета – футляр с гибким магнитным диском.

Дисковод – электромеханическое устройство ЭВМ, обеспечивающее установку, считывание и запись компьютерной информации с дискеты. Является одним из узлов накопителя на гибких магнитных дисках.

Дисплей – электронное устройство отображения видеоинформации. В зависимости от физического метода, используемого для формирования изображения на экране, различают дисплеи с электронно-лучевой трубкой, жидкокристаллические и плазменные.

Документ на машинном носителе – документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Документированная компьютерная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Достоверность передачи информации – соответствие принятого сообщения переданному. Определяет степень вероятности отсутствия ошибок в полученном сообщении.

Доступ к компьютерной информации – всякая форма проникновения к ней с использованием СВТ, позволяющая манипулировать информацией (уничтожать ее, блокировать, модифицировать и копировать). В зависимости от расстояния между местом применения СВТ – средства совершения преступления и местом нахождения компьютерной информации – предмета преступного посягательства, различают дистанционный и непосредственный доступ.

Драйвер – программа для ЭВМ, обеспечивающая автоматическое управление конкретным периферийным устройством (каждому отдельно взятому периферийному устройству соответствует свой драйвер).

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием ее средств, например, ПИН-код.

Интегральная микросхема (ИМС) – микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы, элементы и связи которого неразрывно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие.

Интерпретатор – программа для ЭВМ, совмещающая в себе функции транслятора и компилятора. Пользователь вводит в нее с клавиатуры текст программы, написанной на определенном языке программирования, например, на Бэйсике, и сразу же начинает ее использовать. Входит в состав системы программирования.

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Канал электросвязи – часть сети электросвязи, связывающая между собой источник и приемник сообщений.

Карта оплаты – средство, позволяющее абоненту и (или) пользователю использовать телематические услуги связи, идентифицировав абонента и (или) пользователя для оператора связи как плательщиков.

Каталог (директорий) – справочник файлов и библиотек программ со ссылками на их расположение. Используется операционной системой ЭВМ и пользователем для определения местоположения файла (библиотеки программ). Система каталогов может включать главный (корневой) каталог и подкаталоги (поддиректории).

Код – система условных знаков для передачи, обработки и хранения (запоминания) информации; система условных знаков или сигналов для передачи сведений; программа для ЭВМ, находящаяся в формате машинного языка.

Кодирование – процесс зашифровывания при помощи кода, преобразования в код какой-либо информации в целях ее сбора, хранения, обработки, передачи и использования.

Компилятор (редактор связей) – программа для ЭВМ, позволяющая работать с библиотекой стандартных подпрограмм, которые негласно для пользователя выполняют ввод-вывод данных и команд, их преобразование, математические функции, обращение к операционной системе для работы в которой пишется новая программа, обработку возможных ошибок во время исполнения программы и выдачу сообщений о

них пользователю, остановку исполнения (прерывания) программы по определенным командам, входит в состав системы программирования.

Компьютер – см. *ЭВМ.*

Компьютерная информация – информация, зафиксированная на машинном носителе в форме, доступной восприятию ЭВМ.

Компьютерная технология – система приемов, способов и методов применения средств электронной и вычислительной техники при выполнении функций создания, сбора, обработки, хранения, передачи, использования и уничтожения информации.

Конфигурация – компоновка системы с четким определением характера, количества, взаимосвязей и основных характеристик ее функциональных элементов; совокупность аппаратных средств и соединений между ними; перечень средств, включаемых в данный комплекс или систему.

Конфигурация операционной системы – разновидность версии операционной системы, адаптированной для конкретной ЭВМ.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Концентратор – аппаратное техническое устройство, позволяющее средству передачи данных обслуживать большее количество источников данных по меньшему числу каналов передачи данных.

Копирование компьютерной информации – это повторение и устойчивое запечатление компьютерной информации любыми способами на отличном от оригинала машинном носителе при одновременной сохранности признаков, идентифицирующих ее.

Криптографический протокол – совокупностью действий (инструкций, команд, вычислений, алгоритмов), выполняемых в заданной последовательности двумя или более объектами (субъектами) криптографической системы для достижения следующих целей: обмена ключевой информацией с последующей установкой засекреченного режима передачи и приема сообщений; аутентификации; авторизации. Субъекты криптографической системы – это люди (пользователи), а объекты – автоматы (технические устройства).

Криптография – специальная система изменения открытого письма с целью сделать текст понятным лишь для тех лиц, которые знают эту систему; тайнопись (от греч. «криптос» – скрытый и «графо» – пишу).

Крэкерская атака – действие, целью которого является захват контроля (повышение прав) над удаленной/локальной вычислительной системой, либо ее дестабилизация, либо отказ в обслуживании.

Листинг – распечатка компьютерной информации на твердом физическом носителе (бумаге или пленке).

Логин – имя (идентификатор) учетной записи пользователя в компьютерной системе.

Локальная сеть ЭВМ – сеть ЭВМ, поддерживающая в пределах ограниченной территории (помещения, здания, производственного объекта и т. д.) один или несколько каналов внутрипроизводственной и технологической сети электросвязи для обмена компьютерной информацией.

Локальная сеть ЭВМ – сеть ЭВМ, поддерживающая в пределах ограниченной территории (помещения, здания, производственного объекта и т. д.) один или несколько каналов внутрипроизводственной и технологической сети электросвязи для обмена компьютерной информацией.

Магнитооптический диск – машинный носитель информации, выполненный в виде диска из специального композитного материала. Для записи, чтения и уничтожения информации используется магнитооптический эффект: запись данных выполняется «горячим» лучом лазера и магнитным полем; считывание данных осуществляется «холодным» лучом лазера; уничтожение данных – «горячим» лучом лазера и магнитным полем. Выпускаются диски диаметром 118,5 мм и 80 мм.

Машинный носитель информации – любое техническое устройство либо физическое поле, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации.

Машинограмма – копия электронного документа, распечатанная на бумаге или ином материальном носителе с использованием принтера.

Метка тома – физическая запись на внешнем машинном носителе информации, записываемая на том (диск) при его инициализации (разметке) и содержащая регистрационный номер тома (диска), адрес области меток файлов, идентификатор владельца тома (диска).

Микросхема интегральная (чип, микрочип) – микроэлектронное устройство, электронная схема произвольной сложности (кристалл), изготовленная на полупроводниковой подложке (пластине или пленке) и помещенная в неразборный корпус, или без такового, в случае вхождения в состав микросборки.

Модем – функциональное устройство, обеспечивающее модуляцию и демодуляцию сигналов; преобразующее цифровые сигналы в аналоговую форму и обратно для передачи их по каналам электросвязи.

Модификация компьютерной информации – это внесение в нее любых несанкционированных собственником или владельцем изменений.

Монитор – см. *дисплей*.

Нарушение работы ЭВМ, системы ЭВМ или их сети – это временное или устойчивое создание помех для их функционирования в соответствии с назначением.

Несанкционированный доступ (НСД) – преднамеренное обращение субъекта к компьютерной информации, доступ к которой ему не разрешен, независимо от цели обращения.

Оперативная память – программно-адресуемая память, быстродействие которой соизмеримо с быстродействием центрального процессора; предназначена для хранения исполняемых в данный момент программ и оперативно необходимых для этого данных.

Операционная (мониторная) система (ОС) – совокупность взаимосвязанных программ для ЭВМ, выступающих в качестве интеллектуального посредника между аппаратными средствами ЭВТ, средствами электросвязи системы или сети ЭВМ и пользователем (человеком): командного процессора (интерпретатора команд), драйверов и файловой системы.

Оптический диск – машинный носитель информации, изготовленный в форме диска из тонких полимерных пленок, обладающих различными физическими свойствами. Запись и уничтожение компьютерной информации осуществляется с помощью «горячего» луча лазера, а считывание – «холодного» луча лазера. Различают диски для одноразовой и многоразовой записи информации.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю

информационной системы и предназначенная для подтверждения с использованием средств ЭЦП подлинности этой подписи в электронном документе.

Пакет прикладных программ – набор специализированных программ для ЭВМ, предназначенные для решения задач определенного класса.

Перезагрузка – повторная начальная загрузка операционной системы, выполняемая, как правило, при остановке («зависании») ЭВМ, когда другие способы восстановления ее нормального функционирования не дают положительного результата.

Периферийное устройство (оборудование) – любое техническое устройство, обеспечивающее передачу данных и команд между оперативным или постоянным запоминающим устройством (соответственно ОЗУ и (или) ПЗУ) и пользователем относительно определенного центрального процессора; комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора.

Персональная ЭВМ (персональный компьютер) – универсальная ЭВМ, предназначенная для использования в автономном режиме, системе ЭВМ или их сети для решения задач различной профессиональной ориентации, например, используемая в качестве рабочего места специалиста.

Перфорирование – способ записи компьютерной информации на перфокарту или перфоленту путем пробивки в определенном порядке сквозных отверстий. Осуществляется с помощью специального технического устройства – перфоратора, работающего под управлением ЭВМ.

Печать – процесс передачи компьютерной информации на печатающее устройство (принтер, графопостроитель, плоттер) и получение ее копии на твердом физическом носителе (бумаге, пленке или ином материале).

Пластиковая карта – обобщающее понятие документа, выполненного на основе металла, бумаги или полимерного (синтетического) материала – пластика стандартной прямоугольной формы, хотя бы один из реквизитов которого находится в форме, доступной восприятию средствами электронно-вычислительной техники и электросвязи; имеет стандартные размеры 86×54×0,76 мм.

Плата – сменная панель с электронными приборами и техническими устройствами. «Материнская» плата – основная (базовая) плата, на которой находится центральный процессор, электрические проводники и разъемы для подключения других функциональных плат, а также периферийных устройств.

Пользователь (потребитель) информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Пользователь сертификата ключа электронной цифровой подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Пользователь телематическими услугами связи – лицо, заказывающее и (или) использующее телематические услуги связи.

Порт – многоразрядный вход или выход в техническом устройстве; точка взаимодействия двух технических устройств (например, ЭВМ с принтером); конец логического канала электросвязи.

Предоставление доступа к информационным системам информационно-телекоммуникационной сети – обеспечение возможности приема и передачи телематических электронных сообщений (обмена телематическими электронными сообщениями) между абонентским терминалом и информационной системой информационно-телекоммуникационной сети.

Предоставление доступа к сети передачи данных – совокупность действий оператора связи по формированию абонентской линии, подключению с ее помощью пользовательского (оконечного) оборудования к узлу связи сети передачи данных либо по обеспечению возможности подключения к сети передачи данных пользовательского (оконечного) оборудования с использованием телефонного соединения или соединения по иной сети передачи данных в целях обеспечения возможности оказания абоненту и (или) пользователю телематических услуг связи.

Прикладная программа – программа для ЭВМ, с которой непосредственно работает пользователь для решения вычислительных и информационных задач.

Прикладное программное обеспечение – совокупность прикладных программ для ЭВМ, предназначенных для решения задачи или класса задач в определенной области знания.

Принтер – печатающее устройство, находящееся под управлением ЭВМ.

Программа - оболочка – программа для ЭВМ, облегчающая работу пользователя с операционной системой. Например, «Norton Commander», «Windows Commander» и т. д.

Программа для ЭВМ – это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

Программатор сим-карт – устройство, позволяющее сканировать сим-карты, копировать их содержание на чистые заготовки сим-карт, а также позволяет прошивать мультисим карты, т. е. менять их прошивку.

Программное обеспечение – совокупность входящих в состав системы ЭВМ программных средств. Различают системное программное обеспечение и прикладное программное обеспечение.

Программное средство – программы для ЭВМ, базы данных, служебные данные и документы к ним, обеспечивающие работу ЭВМ, системы ЭВМ или их сети, а также предоставляющие пользователю (потребителю) информации определенные виды обслуживания.

Протокол – результат регистрации в хронологическом порядке информации о ходе вычислительного процесса; в сети ЭВМ – совокупность семантических и синтаксических правил, определяющих работу функциональных устройств в процессе электросвязи.

Протокол обмена – формализованный набор требований к структуре телематического электронного сообщения и алгоритму обмена телематическими электронными сообщениями.

Рабочая станция – компьютер, подключенный к сети ЭВМ и предназначенный для работы пользователя (потребителя информации).

Разметка (форматирование, инициализация) – подготовка машинного носителя информации к использованию путем записи на него служебной компьютерной информации (например, первичная подготовка магнитного диска к работе включает разбиение дорожек диска на сектора, заполнение информационных полей определенным кодом, запись на нулевую дорожку программы начальной загрузки, загрузчика и некоторых системных данных).

Режим разграничения доступа – порядок доступа к компьютерной информации в соответствии с установленными правилами.

Сайт – специализированная программа для ЭВМ, предназначенная для функционирования в глобальной компьютерной сети «Интернет»; обычно состоит из нескольких электронных страниц, содержащих видео-, аудио-, графическую либо текстовую информацию.

Сектор – участок дорожки магнитного диска, являющийся минимальной физически адресуемой единицей памяти.

Сервер 1 – компьютер (или специальное компьютерное оборудование), выделенный и/или специализированный для выполнения определенных сервисных функций (обслуживающий группу компьютеров, как правило объединенных в единую сеть).

Сервер 2 – ЭВМ, выполняющая определенные функции обслуживания пользователей; в сети ЭВМ – управляет использованием разделенных ресурсов (рабочих станций, принтеров, внешней памяти, баз данных, программ для ЭВМ и др.).

Сертификат ключа электронной цифровой подписи – документ на бумажном носителе или электронный документ с ЭЦП уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ ЭЦП и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца ее сертификата.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Сетевой адрес (IP-адрес сокр. от англ. *Internet Protocol Address*) – номер из ресурса нумерации сети передачи данных, однозначно определяющий при оказании телематических услуг связи абонентский терминал или средства связи, входящие в информационную систему.

Сеть ЭВМ – две и более ЭВМ, объединенные между собой с помощью средств электросвязи (электрических проводников, модемов, коммутирующих устройств и т. д.).

Сеть электросвязи – технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания.

Система программирования – пакет инструментальных программных средств, предназначенных для создания программ для ЭВМ.

Система ЭВМ (программно – технический комплекс) – совокупность ЭВМ, программного обеспечения и разнообразных технических устройств (периферийных устройств, управляющих датчиков, исполнительных механизмов и др.), предназначенных для организации и (или) осуществления информационных процессов.

Системное программное обеспечение – совокупность программ, предназначенных для организации работы, эксплуатации и технического обслуживания ЭВМ, системы ЭВМ или их сети, а также автоматизации разработки прикладных программ.

Системный блок – аппаратный блок, содержащий центральный процессор и другие основные технические устройства ЭВМ.

Системный загрузчик – программа для ЭВМ, которая также находится в ПЗУ. Она автоматически включается после исполнения BIOS и производит тестирование всех технических устройств как в самой ЭВМ (интегральных микросхем: ОЗУ, центрального процессора, кэш-памяти и др.; винчестера, дисководов, громкоговорителя и др.), так подключенных к ней (периферийных устройств). При положительном результате тестирования программа запускает на исполнение (загружает) с винчестера или иного машинного носителя операционную систему и передает ей управление ЭВМ. Эта программа также позволяет пользователю выборочно работать с несколькими операционными системами на одной ЭВМ.

Скимминг (от англ. skim – снимать сливки) – установка на банкоматы нештатного оборудования (скиммеров), которое позволяет фиксировать данные банковской карты (информацию с магнитной полосы банковской карты и вводимый пин-код) для последующего хищения денежных средств со счета банковской карты.

Собственник компьютерной информации, информационной системы, технологии и средства их обеспечения – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами.

Спам – телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя.

Спецификация – формализованное описание свойств, характеристик и функций объекта.

Средство защиты информации – техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации.

Средство обеспечения автоматизированной информационной системы и ее технологии – программное, техническое, лингвистическое, правовое или организационное средство (программа для ЭВМ; средство электронно-вычислительной техники и электросвязи; словарь, тезаурус и классификатор; инструкция и методика; положение, устав, должностная инструкция; схема и ее описание, другая эксплуатационная и сопроводительная документация), используемое или создаваемое при проектировании информационной системы и обеспечивающее ее эксплуатацию.

Средство электронно-вычислительной техники (СВТ) – электронное техническое устройство, предназначенное для создания, сбора, хранения, обработки, передачи и (или) уничтожения данных и команд в процессе решения вычислительных и информационных задач.

Средство электронной цифровой подписи – аппаратное и (или) программное средство, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого

ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Средство электросвязи системы или сети ЭВМ – техническое устройство, предназначенное для формирования, передачи и (или) приема, а также регистрации данных и команд (сообщений) в системе либо сети ЭВМ.

Стандартное программное обеспечение – набор определенных лицензированных программ для ЭВМ, поставляемых вместе со средством электронно-вычислительной техники.

Стирание компьютерной информации – частичное уничтожение компьютерной информации с машинного носителя, заключающееся в ликвидации отдельных признаков, позволяющих ее идентифицировать.

Телекоммуникация – дистанционная связь; дистанционная передача данных.

Терминал – техническое устройство для взаимодействия субъекта с системой ЭВМ; в сети ЭВМ (электросвязи) – техническое устройство, являющееся передатчиком либо приемником компьютерной информации (данных, команд, сигналов, сообщений).

Транслятор – программа для ЭВМ, производящая перевод исходного текста программы, написанного человеком на одном из языков программирования (Turbo C, Turbo C++, Turbo Pascal, Microsoft C, Microsoft Basic, Clipper и т. д.), на машинный язык кодов команд (объектный код). Входит в состав системы программирования.

Удаленный доступ – доступ к компьютерной информации, осуществляемый с помощью терминала или рабочей станции.

Уничтожение компьютерной информации – ликвидация компьютерной информации любыми способами без возможности ее восстановления.

Устройство – конструктивно законченная техническая система, имеющая определенное функциональное назначение.

Утечка информации – неправомерный выход охраняемой законом информации за пределы пространства, контролируемого ее правообладателем.

Утилита – см. *вспомогательная программа для ЭВМ.*

Файл – поименованная область записей на машинном носителе информации, где в закодированном виде хранится строго определенная информация с реквизитами, позволяющими ее идентифицировать.

Файловая система – совокупность программ для ЭВМ, обеспечивающих логическое размещение и хранение данных и команд в памяти ЭВМ и на машинных носителях информации в виде логических дисков, папок (каталогов) и файлов.

Файл-сервер – ЭВМ, работающая в локальной сети и содержащая на своих винчестерах прикладные программы и файлы с информацией, обеспечивающие информационные потребности всех пользователей сети.

Физическое поле – материальный носитель физических взаимодействий искусственного или естественного происхождения; особая форма существования материи.

Хакерская атака – мозговой штурм, направленный на нахождение пути решения сложных задач. В хакерской атаке могут принимать участие один или несколько высококлассных специалистов (хакеров). В результате мозгового штурма могут быть придуманы нетрадиционные методы решения проблемы, или внесены оптимизирующие корректировки в уже существующие методы.

Центральный процессор – большая или сверхбольшая интегральная микросхема, выполняющая в ЭВМ основные функции по обработке данных и управлению работой подчиненных периферийных устройств.

Электромагнитный сигнал – средство переноса компьютерной информации в пространстве и во времени с помощью электромагнитных колебаний (волн).

Электронная вычислительная машина (ЭВМ) – программируемое электронное техническое устройство, состоящее из одного или нескольких взаимосвязанных центральных процессоров и периферийных устройств, управление которых осуществляется посредством программ, и предназначенное для автоматической обработки информации в процессе решения вычислительных и (или) информационных задач.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронный ключ (аппаратный ключ) – аппаратное средство, предназначенное для защиты программного обеспечения (ПО) и данных от копирования, нелегального использования и несанкционированного распространения. Основой данной технологии является специализированная микросхема, либо защищенный от считывания микроконтроллер, имеющие уникальные для каждого ключа алгоритмы работы.

Электросвязь – всякая передача или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам.

Учебное пособие

Андреев Алексей Владимирович,
кандидат юридических наук
Аветисян Карен Рафаэлович
Гончар Владимир Владимирович,
кандидат юридических наук
Долбилов Алексей Владимирович,
кандидат экономических наук
Захаров Дмитрий Никанорович,
кандидат технических наук
Иванов Вячеслав Юрьевич,
кандидат технических наук, доцент
Любан Владислав Григорьевич,
кандидат юридических наук
Молянов Алексей Юрьевич,
кандидат юридических наук, доцент
Пузарин Андрей Валерьевич
Русскевич Евгений Александрович,
кандидат юридических наук
Химичева Ольга Викторовна,
доктор юридических наук, профессор

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ ПРОТИВ СОБСТВЕННОСТИ

Научное электронное издание

Редактор *Абилова Ф. А.*
Компьютерная верстка *Абилова Ф. А.*
10,84 усл. печ. л.

Систем. требования: CPU 1,5 Гц; RAM 90,4 МБ; Windows XP SP3;
1 Гб свободного места на жестком диске.

Подписано к изданию 20.04.2020

ISBN 978-5-9694-0845-6

Московский университет МВД России имени В.Я. Кикотя
117437, г. Москва, ул. Академика Волгина, д. 12