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

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Учебное пособие

Москва
2019

ББК 67.408.1
М54

Рецензенты:
заместитель начальника научно-исследовательского центра Академии управления МВД Российской Федерации кандидат технических наук, доцент **А. Л. Ситковский**; старший преподаватель кафедры информационной безопасности Краснодарского университета МВД России кандидат технических наук, доцент **Е. С. Поликарпов**

Коллектив авторов:
И. Г. Чекунов, И. А. Рядовский, А. В. Пузарин, Р. Р. Сабитов, Е. А. Русскевич, С. Ю. Голованов

М54 Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / [И. Г. Чекунов и др.]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2019. – 176 с.
ISBN 978-5-9694-0802-9

В пособии подробно разобрана характеристика компьютерных преступлений. Выделены орудия и средства совершенствования компьютерных преступлений. Классифицировано вредоносное программное обеспечение, выступающее в том числе и средством совершения компьютерного преступления. Проработаны аспекты хищения в электронных платежных системах, включая способы совершения подобных преступлений в электронных платежных системах.

ББК 67.408.1

ISBN 978-5-9694-0802-9

ОГЛАВЛЕНИЕ

Введение..... 5
Глава 1. Международные правовые акты о противодействии киберпреступности..... 7
1.1. Европейская конвенция о киберпреступности..... 7
1.2. Иные международно-правовые акты противодействия киберпреступности..... 9
Глава 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации и особенности квалификации хищений, совершаемых с использованием информационно-коммуникационных технологий..... 12
2.1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)..... 13
2.2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)..... 28
2.3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (ст. 274 УК РФ)..... 43
2.4. Неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274.1 УК РФ)..... 51
2.5. Особенности квалификации хищений, совершаемых с использованием информационно-коммуникационных технологий (п. «г», ч. 3 ст. 158, ст. 159.3, ст. 159.6 УК РФ)..... 60
Глава 3. Криминалистическая характеристика компьютерных преступлений..... 83
3.1. Орудия и средства совершения преступлений..... 83
3.2. Вредоносные программы и их подвиды..... 85
3.3. Классификация троянских программ..... 89
3.4. Программно-аппаратные устройства..... 94
3.5. Отдельные виды компьютерных преступлений..... 96

Глава 4. Хищения в электронных платежных системах 103
4.1. Способы совершения преступлений в электронных платежных системах 103
4.2. Функциональные возможности современных вредоносных программ 105
4.3. Методы сокрытия следов преступления 117
4.4. Следственные версии по делам о хищениях в платежных системах 121
4.5. Лица, совершающие преступления в сфере компьютерной информации 122
4.6. Причины и условия совершения преступлений 124
Глава 5. Кибертерроризм 128
Глава 6. Особенности сбора доказательств по делам о компьютерных преступлениях 140
6.1. Источники доказательств 140
6.2. Следственные действия 143
6.3. Использование в доказывании результатов оперативно-разыскной деятельности 146
6.4. Требования к специалисту, привлекаемому к сбору доказательств 148
6.5. Проблемы сбора доказательств на современном этапе 150
Глава 7. Тактические особенности производства некоторых следственных действий 153
7.1. Общие принципы работы с электронными доказательствами ... 153
7.2. Осмотр места происшествия 155
7.3. Производство обыска 158
7.4. Допрос 160
7.5. Судебная компьютерная экспертиза 162
7.6. Типичные ошибки при проведении обыска или осмотра и назначении экспертизы 164
Глава 8. Опережающие технологии в сфере противодействия киберпреступности: KSN – Сеть обеспечения безопасности 166
Заключение 175

ВВЕДЕНИЕ

В настоящее время все большее количество государств ставит перед собой в качестве приоритетной цели создание информационного общества на основе широкого внедрения телекоммуникационных технологий. Одной из определяющих задач на этом пути является системное развитие и внедрение цифровых технологий во всех областях жизни.

В соответствии с утвержденной распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р программой «Цифровая экономика Российской Федерации» и «дорожными картами» по направлениям ее реализации, к 2024 г. 97 % домохозяйств в России должны иметь широкополосный доступ к интернету (100 Мбит/с), информационные системы и ресурсы органов государственной власти и местного самоуправления должны быть перенесены в государственную единую облачную платформу в полном объеме, доля внутреннего сетевого трафика российского сегмента интернета, маршрутизируемая через иностранные серверы, и стоимостная доля закупаемого или арендуемого федеральными органами исполнительной власти, органами исполнительной власти субъектов, государственными корпорациями, компаниями с государственным участием иностранного программного обеспечения (далее – ПО) должны составить не более 10 %.

В России должно появиться 10 компаний – технологических лидеров, конкурентоспособных на глобальных рынках в сфере высоких технологий, и такое же количество цифровых платформ для основных отраслей экономики.

Будет создано не менее 50 аспирантских и магистерских школ по направлениям «сквозных» технологий на базе ведущих вузов и научных организаций, а «доля населения, обладающего цифровыми навыками», предположительно, составит 40 %.

Постановка таких задач вполне оправданна, поскольку сегодня компьютеры, мобильные средства связи, их ПО, телекоммуникационные системы и технологии охватывают практически все сферы жизнедеятельности человека, общества и государства. В то же время вместе с развитием информационного пространства необходимо активизировать усилия общества по его защите от преступных посягательств, совокупность которых уже имеет свое собственное, известное во всем мире название – киберпреступность. Она успела

получить широкое распространение и в современных условиях составляет одну из наиболее опасных угроз для общества.

Изложенные выше обстоятельства обусловили необходимость подготовки настоящего пособия, первое издание которого вышло в 2018 г. За прошедший год произошли изменения в российском законодательстве, в первую очередь в Уголовном кодексе Российской Федерации, что потребовало отражения в пособии. В результате новое издание было дополнено отдельной главой, содержащей детальную уголовно-правовую характеристику преступлений в сфере компьютерной информации, рассмотрение особенностей квалификации хищений, совершаемых с использованием информационно-коммуникационных технологий, а также подробный анализ изменений, внесенных в ст.ст. 158, 159.3 и 159.6 УК РФ. Кроме того, во втором издании обновлены данные о способах совершения хищений с использованием информационно-коммуникационных технологий, актуализирован параграф об отдельных видах компьютерных преступлений и, учитывая запрос времени, введена новая глава об опережающих информационных технологиях противодействия киберпреступности на примере созданной «Лабораторией Касперского» и успешно развивающейся технологии *Kaspersky Security Network* (также – *KSN*).

ГЛАВА 1. МЕЖДУНАРОДНЫЕ ПРАВОВЫЕ АКТЫ О ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

1.1. Европейская конвенция о киберпреступности

Одним из первых международных правовых актов, рассматривающих вопросы борьбы с киберпреступлениями, стала Конвенция Совета Европы о преступности в сфере компьютерной информации, принятая в Будапеште в 2001 г.

Несмотря на то, что в Конвенции упоминается термин «киберпреступление», а не «компьютерное преступление» либо «преступление в сфере компьютерной информации», от его трактовки в тексте документа авторы отказались. Вместо этого они разработали классификацию киберпреступлений, распределив их по четырем группам. Позднее, в соответствии с принятым 28 января 2003 г. в Страсбурге дополнительным протоколом, классификация была дополнена еще одной группой.

К первой группе отнесены преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

– незаконные доступ к компьютерной системе или любой ее части и перехват компьютерных данных;

– незаконное повреждение, стирание, порча, изменение или блокирование компьютерных данных;

– незаконное умышленное нарушение функционирования компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или блокирования компьютерных данных;

– производство, приобретение с целью использования и распространение технических средств, в том числе компьютерных программ и иных данных, предназначенных для совершения любого из указанных преступлений.

Вторую группу составляют преступления, связанные с использованием компьютерных средств:

– подлог с использованием компьютерных технологий путем введения, изменения, стирания или блокирования компьютерных данных;

– мошенничество с использованием компьютерных технологий путем введения, изменения, стирания, блокирования компьютерных данных либо вмешательства в функционирование компьютерной системы.

Преступления, связанные с контентом, в первую очередь – детской порнографией, представлены в третьей группе:

– изготовление, распространение и получение материалов, связанных с детской порнографией, через компьютерную сеть;

– обладание такими материалами в компьютерной системе или на носителе компьютерных данных.

В четвертую и пятую группы включены преступления, связанные с нарушениями авторского права и смежных прав, и преступления, связанные с распространением информации расистского и ксенофобского характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц под предлогом расовой, национальной, религиозной или этнической принадлежности.

Присоединившиеся к Конвенции страны-участники гарантировали, что национальными законами будет обеспечена уголовная наказуемость за перечисленные выше деяния.

При разработке процедур межгосударственного взаимодействия, связанного с обнаружением, фиксацией и изъятием компьютерных данных, авторы Конвенции исходили из того, что киберпреступность по своей сути трансгранична, поэтому и борьба с ней должна иметь соответствующий глобальный характер. В связи с этим были предложены процедуры по поиску, обнаружению, фиксации и изъятию компьютерных данных, которые страны-участники могли бы включить в национальные уголовно-процессуальные законы и регламенты, а также упрощенный порядок межгосударственного взаимодействия при осуществлении таких мероприятий.

Универсальным правовым документом мирового масштаба Конвенция не стала. Россия, наряду со многими другими государствами, отказалась от присоединения к ней, а многие положения Конвенции на протяжении всего времени ее действия с момента вступления в силу в 2004 г. подвергались критике, в том числе в связи с тем, что они не смогли разрешить имеющиеся и вновь возникающие проблемы международного сотрудничества в сфере борьбы с киберпреступлениями.

Конвенция создавалась почти 20 лет назад, все это время развитие технологий в информационно-коммуникационной сфере продолжалось бурными темпами, оцифровывая все новые сферы человеческой жизнедеятельности. Эти обстоятельства не могли не повлиять и на такое негативное явление, как преступность. Наверное, уже не оста-

лось уголовно наказуемого деяния, по которому отсутствовал бы прецедент, связанный с использованием в качестве средств совершения преступления коммуникационных сетей, вычислительной техники и компьютерных программ. Классификация киберпреступлений по пяти группам, предложенная в свое время авторами Конвенции, уже не отвечает современным реалиям и требует переосмысления.

Тем не менее Конвенция сыграла и продолжает играть значительную роль в развитии международных правовых инструментов противодействия киберпреступности и совершенствовании национальных уголовных законов в этой сфере.

1.2. Иные международно-правовые акты противодействия киберпреступности

Наряду с рассмотренной выше Конвенцией Совета Европы на международном уровне 1 июня 2001 г. принят еще один документ противодействия киберпреступности – Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации.

Задачи, которые стояли перед разработчиками обоих международных актов, были одинаковыми: принять единообразную классификацию преступлений в сфере компьютерной информации, предложить меры противодействия таким преступным проявлениям, которые были бы востребованы странами-участниками, и обеспечить эффективное межгосударственное взаимодействие при расследовании уголовных дел.

Однако Соглашение по сравнению с Конвенцией рассматривает область борьбы с преступлениями в сфере компьютерной информации в более узком смысле. Это отражено в первой же статье документа, в которой дано определение термина «преступление в сфере компьютерной информации», согласно которому под ним понимается уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация. Таким образом, из данной группы были исключены деяния, в которых компьютерная информация и электронно-вычислительные устройства используются исключительно в качестве средств либо орудий совершения преступления, но не являются предметом преступного посягательства. В рамках этого определения предусмотрена и классификация таких преступлений:

– осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение,

блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

– создание, использование или распространение вредоносных программ;

– нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;

– незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

Перечень и состав преступлений практически полностью совпадает с первой редакцией главы 28 УК РФ. Классификация дополнена описанием лишь еще одного деяния, связанного с нарушением авторского права по отношению к компьютерным программам и базам данных, которое, очевидно, охватывается диспозицией ст. 146 «Нарушение авторских и смежных прав» Уголовного кодекса Российской Федерации.

Мероприятия по межгосударственному взаимодействию при расследовании преступлений в сфере компьютерной информации, предусмотренные Соглашением, носят общий характер, без регламентации конкретных процедур по поиску, обнаружению, фиксации и изъятию доказательств.

Тем не менее, несмотря на все недостатки, Соглашение как первый международный правовой документ, разработанный в целях противодействия киберпреступности, безусловно, является важным этапом в формировании международных и национальных правовых актов в этой сфере.

Другие международные правовые акты, в рамках которых осуществляется межгосударственное взаимодействие в связи с расследованием преступлений в сфере компьютерной информации, являются универсальными с точки зрения оказания правовой помощи по уголовным делам:

– Европейская конвенция о взаимной правовой помощи по уголовным делам, принятая 20 апреля 1959 г.;

– Минская конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам, принятая 22 января 1993 г.

Россия присоединилась к обеим конвенциям и активно взаимодействует с другими странами-участниками в интересах совместной борьбы с криминалом. Однако проверенные временем и хорошо проработанные процедуры оказания правовой помощи по так называемым традиционным преступлениям оказываются малоэффективными при расследовании преступных посягательств в сфере компьютерной информации. Длительный процесс обмена бумажными документами по официальным каналам не в состоянии обеспечить оперативное принятие решений о сохранении данных, обрабатываемых и передающихся компьютерными системами и их сетями, в результате чего доказательства по уголовным делам, имеющим трансграничный характер, могут быть безвозвратно утрачены.

Резюмируя изложенное, приходится признать, что в настоящее время международное сообщество не выработало универсального правового акта, обеспечивающего эффективное межгосударственное сотрудничество в сфере противодействия киберпреступности. Действующие конвенции либо носят региональный характер, либо не отвечают специфическим требованиям к процессу сбора цифровых доказательств.

ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ОСОБЕННОСТИ КВАЛИФИКАЦИИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

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 отметить, что практику их применения до настоящего времени нельзя признать удовлетворительной, хоть в малой степени соответствующей современному размаху криминальной активности в виртуальном пространстве.

По данным Главного информационно-аналитического центра МВД России, динамика преступлений, предусмотренных главой 28 УК РФ, представлена следующим образом (*рис. 2.1*):

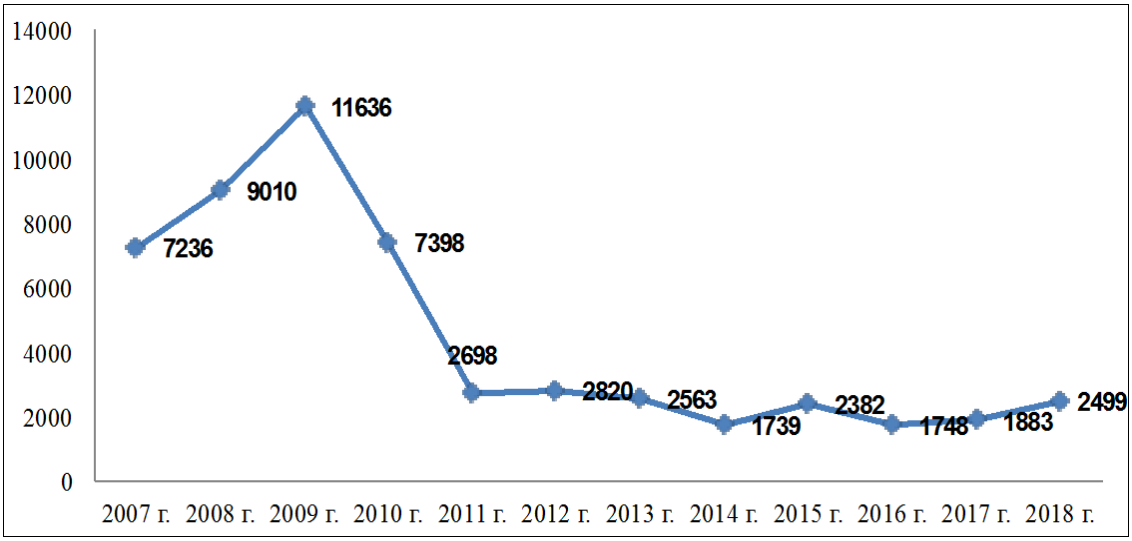


Рис. 2.1. Количество преступлений по статьям, включенным в главу 28 УК РФ

[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, и др.

2.1. Неправомерный доступ к компьютерной информации (ст. 272 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.

Динамика преступлений, предусмотренных ст. 272 УК РФ, представлена следующим образом (*рис. 2.2*):

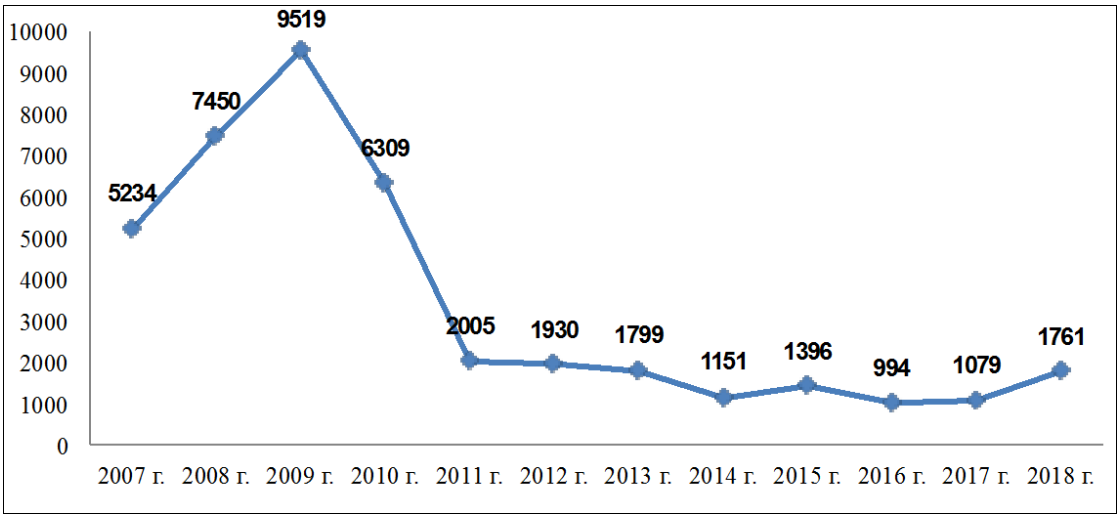


Рис. 2.2. Количество преступлений по ст. 272 УК РФ

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

В теории уголовного права нет общепринятой позиции относительно ключевого вопроса о том, что следует понимать под охраняемой законом информацией[1]. Высказана та 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].

---

[1] Следует отметить, что законодательства ряда стран используют более общую категорию – «информация, хранящаяся в компьютерной системе, сети или на машинных носителях». Напр.: Швед Н. А. Неправомерный доступ к компьютерной информации: уголовно-правовая защита в РФ 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.

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. [1] 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.)[2].

Отсутствие общепринятого толкования термина «охраняемая законом информация» закономерно обусловило неединообразную практику применения ст. 272 УК РФ. Отдельные суды, придерживаясь рекомендаций Генеральной прокуратуры РФ, указывают, что неправомерные манипуляции с открытой (общедоступной) информацией не подпадают под действие данной статьи.

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 июля 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

---

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

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

и 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.

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,

---

[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.

направленных на: 1) обеспечение защиты 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 Минкомсвязи России от 27 июня 2013 г. № 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами 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

---

[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. 23 авг. (№ 187).

Правил размещения на официальном сайте образовательной организации информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации»[1].

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 разнообразными (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 и 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 скорее как ее сокрытие от посторонних, при котором применение специальных методов позволяет эти данные восстановить. При уничтожении информация восстановлению не подлежит[2].

---

[1] Собр. законодательства Рос. Федерации. 2013. 22 июля (№ 29). Ст. 3964.

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

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 в компьютерную информацию любых изменений, которые обусловят ее отличие от ранее хранившейся в компьютерной сети, системе или на машинном носителе собственника информационного ресурса, в результате чего потерпевшему будет причинен имущественный ущерб, а виновное лицо извлечет из этого выгоду[1].

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[2].

Сомнительно утверждать об отсутствии в такой ситуации причинно-следственной связи между действиями лица и наступившими общественно опасными последствиями в виде копирования охраняемой законом компьютерной информации. Думается, что такая связь объективно имеется.

С другой стороны, неосведомленность лица об особенностях настроек программы фактически исключает вину по отношению

---

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

[2] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] // СПС «Консультант-Плюс».

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 скиммингового оборудования также квалифицируются по ст. 272 УК РФ.

Б. совершил неправомерный доступ к охраняемой законом компьютерной информации – информации на машинном носителе, – повлекший копирование информации, из корыстной заинтересованности при следующих обстоятельствах. Б. приобрел в не установленном следствием месте у неустановленного лица скимминговое оборудование в виде накладки на кардридер банкомата для тайного несанкционированного считывания информации с банковских карт, представляющего 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 скиммингового 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 скиммингового 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 рубля.

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 держа-

телем банковской карты при наборе на клавиатуре ПИН-кода для доступа к своему банковскому счету, что повлекло несанкционированное копирование информации, выразившееся в переносе в память скиммингового 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.

---

[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 [Электронный ресурс] // СПС «Консультант-Плюс».

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 1 млн рублей. С качественной стороны ущерб может выражаться как в прямых имущественных потерях обладателя информации (например, расходы, связанные с восстановлением уничтоженного или модифицированного ПО), 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 для других лиц.

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 с использованием сетевых реквизитов, принадлежащих его родному брату (что было вызвано 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 «рое-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 – обеспечить себе бесплатный доступ к сети Интернет, при помощи персонального компьютера, подключенного

к сети Интернет посредством оператора связи, осознавая, что имеющиеся 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 «рое-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 Мб стоимостью 1 699, 63 рубля[1].

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

Сотрудниками управления «К» МВД России была пресечена деятельность организованной группы, которая специализировалась

---

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

на взломе аккаунтов в различных соцсетях, почтовых серверах и веб-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 субъекта неправомерного доступа 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 выполнен устойчивой группой лиц, заранее объединившейся для совершения одного или нескольких преступлений.

Использование своего служебного положения предполагает доступ к охраняемой законом компьютерной информации благодаря за-

---

[1] Задержаны хакеры, взламывавшие по заказам страницы в соцсетях, почтовые ящики и занимавшиеся «прослушкой» [Электронный ресурс] // URL: https://мвд.рф/news/show_102385 (дата обращения: 26.08.2016).

[2] Как известно, данная позиция нашла свое неоднократное подтверждение в решениях Верховного Суда Российской Федерации, напр.: постановление Президиума Верховного Суда Российской Федерации № 436п96 по делу Ткаченко В. П. и Хоперского В. В. // Бюллетень Верховного Суда Российской Федерации. 1997. № 4 ; постановление Президиума Верховного Суда Российской Федерации № 495п03 по делу Бычкало и др. // Бюллетень Верховного Суда Российской Федерации. 2004. № 3 и др.

нимаемому 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.

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].

---

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

[2] Так, приказом МВД России № 1144 от 3 декабря 2007 г. «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 от-

 *При 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*[1].

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.

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.

ветственности 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).

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

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

---

[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 и др.

документа как предмета преступления, отметим, что в силу положений ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «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.

Часть 4 ст. 272 УК РФ предусматривает два особо квалифицирующих признака: неправомерный доступ к охраняемой законом компьютерной информации признается осуществленным, 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 вреда здоровью средней тяжести 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.

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

В наше время, пожалуй, трудно найти пользователя современнымх информационно-коммуникационных технологиямий, 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»[1] или «кибероружие»[2].

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 лицам, коммерческим организациям и правительственным учреждениям, в более чем 150 странах мира[3].

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 по-

---

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

[2] Казарин О. В., Шаряпов Р. А. Вредоносные программы нового поколения – одна из существующих угроз международной информационной безопасности // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2015. № 12 (155). С. 9–23 ; Stefano Mele. Legal consideration on cyber-weapons and their definition // Journal of Law & Cyber Warfare, Volume 3, Issue 1, 2014. P. 53.

[3] Владимир Путин назвал спецслужбы США источником вируса WannaCry [Электронный ресурс] // URL: http://www.kommersant.ru/doc/3297338 (дата обращения: 20.11.2017).

нимания вредоносной программы как конструктивного признака ст. 273 УК РФ.

Динамика преступлений, предусмотренных ст. 273 УК РФ, представлена следующим образом (*рис. 2.3*):

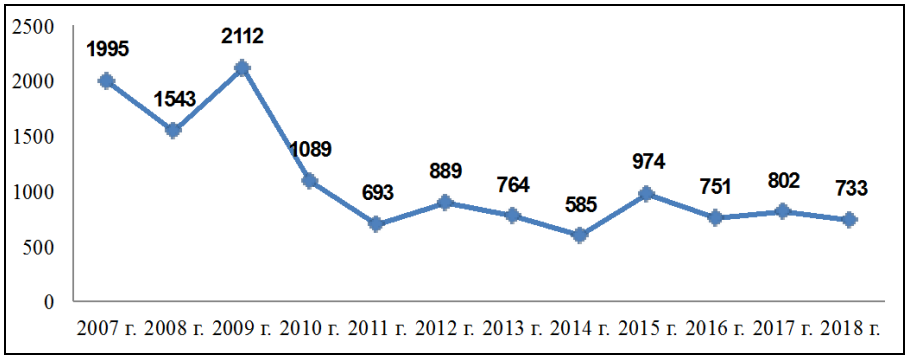


Рис. 2.3. Количество преступлений по ст. 273 УК РФ

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[1].

В этом же ключе содержание вредоносной программы раскрывается в пп. 2.6.5. и 2.6.6. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст[2] «Об утверждении государственного стандарта». 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

---

[1] Собрание законодательства Российской Федерации. 2009. 30 мар. (№ 13). Ст. 1460.

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

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: 1) программа способна уничтожать, блокировать, модифицировать либо копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации; 2) программа не предполагает предварительного уведомления собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети о характере своих действий; 3) 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.).

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 работоспо-

[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.

собности 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[1].

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

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 компьютера Маликова обнаружены комплексы вредоносного ПО, предназначенного для построения «ботнетов» («бот-сетей»), то есть сетей из зараженных соответствующим вирусом компьютеров

---

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

с возможностью удаленного копирования информации назначенным владельцем указанной сети без ведома пользователя и без получения его согласия на применение указанных программ. Работа обнаруженного на жестком диске вредоносного ПО построена на использовании вирусов типа «троян» («троянская программа»)[1].

Господствующее толкование вредоносности компьютерной программы, к сожалению, имеет свои изъяны. Так, 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 ПО. 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

---

[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 и т. п. – в зависимости от «чувства юмора» автора такой программы. К этому классу также относятся программы, предназначенные для мошенничества, например, путем распространения архивов с оплатой за SMS // URL: https://threats.kaspersky.com/ru/threat/Hoax.JS.BadJoke (дата обращения: 22.11.2017).

неправомерных или даже преступных действий (хищения денег с банковских счетов, укрытия средств от налогообложения, хулиганства и т. д.)»[1].

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[2].

Пункт 2 «Правил оказания телематических услуг связи», утвержденных постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575, вредоносное ПО 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[3].

Если исходить из подобного, более широкого понимания вредоносности как предназначения программы к заведомо противоправной (преступной) деятельности в целом, то изготовление и распространение программ-шпионов, *Bad Jokes* 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»[4]) убедительно свидетельствует в пользу именно этого подхода. С течением времени вредоносные программные продукты все больше будут направлены не на отноше-

---

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

[2] 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.

[3] Собр. законодательства Российской Федерации. 2007. 17 сент. (№ 38). Ст. 4552.

[4] 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., 2016. С. 296.

ния 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[1]. Полагаем, что автор необоснованно смешивает вредоносные программы и легальное ПО, 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, программы для записи дисков (*InfraRecoder, BurnAware, Nero* и др.) используются злоумышленниками для изготовления контрафактной продукции (неправомерного копирования информации), ПО 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 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 ПО обладает уже другими характеристиками, напрямую указывающими на ее предназначение для осуществления противоправной деятельности.

---

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

Следует упомянуть об общепринятом в доктрине уголовного права положении: вредоносность ПО – категория юридическая, 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:

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

б) использование таких компьютерных программ или такой компьютерной информации;

в) 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 ПО отнюдь не предполагает, что лицо обладает профессиональными навыками программирования. Созданием также будет являться получение вредоносного программного продукта в результате использования так называемых конструкторов вирусов.

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 вредоносной 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 (далее – ОС) семейства Microsoft Windows. 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 рублей 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.

---

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

 *Абросов с помощью своего компьютера, подключенного к информационно-телекоммуникационной сети Интернет через провайдера, умышленно, с целью блокирования компьютерной информации, используя вредоносную компьютерную программу «ХОИ К», заведомо предназначенную для несанкционированного блокирования компьютерной информации, осуществил компьютерную атаку типа «отказ в обслуживании» на сайт, принадлежащий официальному сайту Президента Российской Федерации*[1].

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

 *Карташов с целью обеспечения эксплуатации без ограничения по времени программного продукта Microsoft Office Professional 2007 Russian, правообладателем которого является Microsoft Corporation, без активационного ключа правообладателя замыслил 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 одного экземпляра программного продукта Microsoft Office Professional 2007 Russian. Затем Карташов во время 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*

---

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

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 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.

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 без-

---

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

возмездного 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 способом 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

---

[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 [Электронный ресурс] // СПС «Консультант-Плюс».

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.

Зинченко, оказывая услуги по установке контрафактного ПО, *подсоединил к системному блоку компьютера имеющийся у него внешний жесткий диск WesternDigital, на котором хранилась программа «1С:Предприятие, версия 8.2», установил на жесткий диск D персонального компьютера файлы программы «1С:Предприятие, версия 8.2». Затем для изменения конфигурации программы «Управление производственным предприятием» воспользовался программой EmulSmallx32Setup.exe – патчем, предназначенным 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 рублей (1 купюра достоинством 5 000 рублей, 2 купюры достоинством 1 000 рублей каждая, 2 купюры достоинством 100 рублей каждая) и передал их Зинченко за оказанную услугу. После чего Зинченко убрал данные денежные средства в карман своей одежды, отсоединил от персонального компьютера*

свой внешний жесткий диск WesternDigital 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, 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), имеющий 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 рублей.

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 рублей.

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. В разделе свойств файла в дате записи на внутренний жесткий диск № Z3T4LKLP системного блока указаны данные: 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\Crac

k имеется файл программы EmulSmallx32Setup.exe. В разделе свойств файла в дате записи на переносной жесткий диск S/NWXE607647066 системного блока указаны данные: 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.

---

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

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.

2.3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (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.

Приведена динамика преступлений, предусмотренных ст. 274 УК РФ (*рис. 2.4*).

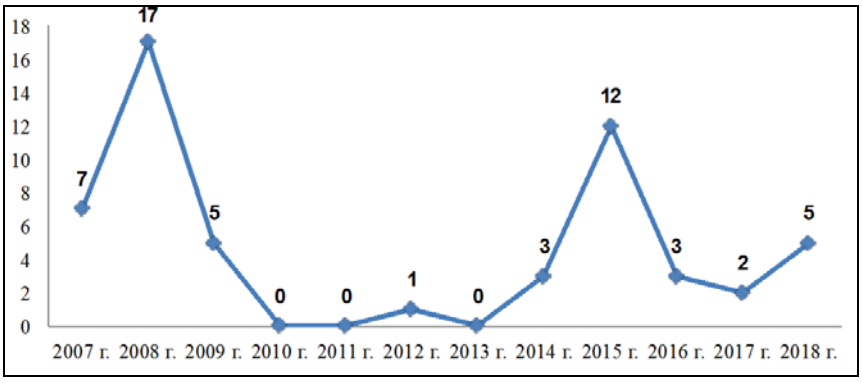


Рис. 2.4. Количество преступлений по ст. 274 УК РФ

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, обработки или

---

[1] Лопашенко Н. А. Уголовно-правовая и криминологическая политика государства в области высоких технологий [Электронный ресурс] // URL: http://sartraccc.ru/i.php?filename=Pub%2Flopashenko%2830-06%29.htm&oper=read_file (дата обращения: 10.05.2017).

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 наиболее четкого определения их перечня.

Прежде всего такие правила устанавливаются на уровне нормативных правовых актов. В качестве примера можно привести постановление Правительства РФ от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи»[2], приказ Министерства связи и массовых коммуникаций РФ 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.).

---

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

[2] Собр. законодательства Рос. Федерации. 2007. 17 сент. (№ 38). Ст. 4552.

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

По одному из дел суд обоснованно указал, что «…правила эксплуатации клиентом устройства самообслуживания определяются 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»[1].

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 устанавливать прикладное, операционное, сетевое и другие виды ПО, 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 ресурсам сети Интернет, 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.

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 ПО *рабочих станций с серверов (п. 2.6), обеспечивает своевременное копирование, архивирование и резервирование данных (п. 2.8), обеспечивает*

---

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

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 ПО; несанкционированная модификация ПО; 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 уров-

ня 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 являются 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 1 млн рублей). 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.

Анисимов, замышляя нарушение правил эксплуатации средств хранения и передачи охраняемой компьютерной информации, повлекшее копирование компьютерной информации, находясь на своем рабочем месте, используя средства авторизации (логин и па-

роль) 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 06 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 40 000 записей, содержащих не прошедшие проверку имена, фамилии, никнеймы (имена, которые используются при регистрации на интернет-сайтах), а также адреса электронной почты.

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

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 рублей);

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

– средний простой 115 сотрудников, имеющих доступ к *VPN*-серверам, из-за необходимости перенастройки *VPN*-серверов составил 12 часов, то есть суммарно 920 часов на ожидание восстановления доступа к *VPN*-серверам, которые были оплачены организацией (общие затраты – 414 000 рублей);

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

– 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 рублей).

Таким образом, Анисимов нарушил правила эксплуатации средств хранения и передачи охраняемой компьютерной информации, скопировав компьютерную информацию, чем причинил крупный вред юридическому лицу на общую сумму 1 155 600 рублей[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.

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

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], в котором глава 28 УК РФ была дополнена специальной нормой об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274.1).

---

[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. 31 июл. (№ 167).

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, в ряду квалифицирующих признаков совершения компьютерных преступлений Уголовного кодекса Азербайджанской Республики 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]. Новый Уголовный кодекс 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

---

[1] Уголовный кодекс Азербайджанской Республики от 30 декабря 1999 г. № 787-IQ (с изм. и доп. по сост. на 31.05.2016 г.) [Электронный ресурс] // URL: http://online.zakon.kz/m/Document/?docid=30420353#sub_id=2710000 (дата обращения: 07.11.2017).

[2] Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V (с изм. и доп. по сост. на 11.07.2017 г.) [Электронный ресурс] // URL: http://online.zakon.kz/m/Document/?doc_id=33885902 #sub_id=320200 (дата обращения: 07.11.2017).

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[1].

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, выход из строя критически важной информационной инфраструктуры (*critical information infrastructure breakdown*) назван среди наиболее актуальных угроз мировой экономике[2], в связи с чем информационные ресурсы стратегического значения, связанные с обеспечением общественной и государственной безопасности, должны быть действенно и эффективно защищены, в том числе 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 преступ-

---

[1] Осужден томский хакер, взломавший сайт Президента РФ // РИА Новости. 2013. 23 дек.

[2] The Global Risks Report 2016 [Электронный ресурс] // URL: http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/world-economic-forum-global-risk-report-2016.pdf (дата обращения: 27.06.2017).

ного посягательства на безопасность компьютерных данных и систем: 1) неправомерный доступ; 2) создание и распространение вредоносного контента; 3) 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 ею 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 уста-

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

новлена только в случае уникальности средств и технологий программной защиты объектов критической информационной инфраструктуры, что представляется маловероятным.

Специфическим предметом преступлений, предусмотренных чч. 2–3 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, атомной, ракетно-космической, горнодобывающей, металлургической 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: создания, использования или распространения 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 конкретного 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 компью-

---

[1] Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет : монография. М., 2015. С. 37 ; Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учебное пособие. М., 2017. С. 44.

терной информации, заведомо предназначенных 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[1].

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 ПО, 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

---

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

целей изготавливается данная программа, содеянное необходимо квалифицировать как пособничество в совершении неправомерного доступа, то есть по ч. 5 ст. 33 и ч. 2 ст. 274.1 УК РФ.

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

1) 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;

2) 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. 1–2 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 Н. Ш. Козаева, считавшего, 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. 4–5 ст. 274.1 УК РФ, являются традиционными для преступлений в сфере компьютерной информации и в целом хорошо освещены в современной литературе[2]. Дискуссионными, пожалуй, можно назвать два реализованных решения. Во-первых, законодатель проявил малопонятную последовательность в регламентации совершения преступления предварительно сговорившейся и организованной группы 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

---

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

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

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.

2.5. Особенности квалификации хищений, совершаемых с использованием информационно-коммуникационных технологий (п. «г» ч. 3 ст. 158, ст. 159.3, ст. 159.6 УК РФ)

Стремительная «цифровизация»[1] отечественной экономики помимо положительных аспектов с точки зрения повышения ее эффективности и конкурентоспособности имеет, к сожалению, и свою негативную (криминогенную) сторону. Уязвимости внедряемых в финансово-кредитную сферу инновационных технологий активно

[1] 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 и др.

эксплуатируют преступники, совершая посягательства на имущество граждан и организаций 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, средняя сумма убытков в одной компании составила 299 940 рублей. В целом по стране потери от атак, совершаемых с использованием современных информационно-коммуникационных технологий, оцениваются на сумму свыше 116 млрд рублей[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

---

[1] Российские компании потеряли не менее 116 млрд рублей от кибератак в 2017 году // [Электронный ресурс] // URL: https://www.nafi.ru/analytics/rossiyskie-kompanii-poteryali-ne-menee-116-mlrd-rubley-ot-kiberatak-v-2017-godu (дата обращения: 30.06.2018).

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

платежные карты, но и иные современные средства безналичных расчетов с использованием информационно-коммуникационных технологий (*Apple Pay, Samsung Pay* и др.)[1].

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[2]. 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 предоставляет правоприменителям возможность задействовать весь спектр оперативно-разыскных мероприятий[3].

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 информа-

---

[1] 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, позволяющие 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.

[2] [Электронный ресурс] // URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=159733&rnd=4C4C85B84AD6F5C60364116A6485AEF6#006814073483298333 (дата обращения: 05.07.2018).

[3] 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.

ции, 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 абза-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[1]. Как представляется, проблема оценки манипуляций с компьютерной информацией как особого рода обмана имеет искусственный характер и обусловлена изначально неудачной редакцией ст. 159.6 УК РФ. Название данной нормы, к сожалению, представляет собой неадаптированный к российской правовой системе и почти автоматизированный перевод ст. 8 «Компьютерное мошенничество» (*Computer fraud*) Конвенции «О преступности в сфере компьютерной информации» (г. Будапешт, 23 ноября 2001 г.)[2]. Учитывая многовековую

---

[1] Заседание Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. // Электронный ресурс: http://www.vsrf.ru/press_center/news/26093 (дата обращения: 06.12.2017).

[2] Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 г. // режим доступа: СПС «Консультант-Плюс».

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, 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 РФ, *в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «Мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия квалифицируют как кражу, если виновным не было оказано незаконного воздействия на ПО серверов, компьютеров или на сами информационно-телекоммуникационные сети*. Таким образом, новые формы посягательства преимущественно на электронные денежные средства граждан Пленум предложил квалифицировать по-старинке – 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 осознававших противоправный характер совершаемых действий, содеянное необходимо будет квалифицировать как грабеж.*

Более того, *если возможность воспользоваться телефоном потерпевшего возникла в результате нападения, сопряженного с при-*

---

[1] Уголовный кодекс Республики Беларусь: с изм. и доп. на 05.01.2015 г. Минск : Нац. центр правовой информ. Респ. Беларусь, 2015. С. 98.

менением насилия, опасного для жизни или здоровья потерпевшего либо с угрозой его применения, и манипуляции с услугой мобильного информирования 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 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 *SIM*-карт и использования вредоносного ПО. С учетом последних разъяснений Пленума хищения денежных средств граждан и организаций в результате использования вредоносных компьютерных программ следует оценивать как мошенничество в сфере компьютерной информации.

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. Указанные программы предназначены для управления удаленным компьютером по сети. После этого Бузин отправил на адрес электронной почты, используемой 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 легально-

го 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 банковском счете и находящихся на нем денежных средствах, 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 ПО, что само по себе не исключает необходимость квалификации содеянного по ст. 159 УК РФ.*

---

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

 *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 ОС 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:

1. Редакционная коллегия отметила, что высокий уровень развития товарно-денежных отношений, информационных технологий и банковских услуг позволяет за считанные минуты осуществлять пе-

---

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

ревод 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 беспрепятственно распоряжаться ими.

2. 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[1].

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 ПО служебного компьютера организации с установленной системой «Банк-Клиент»[2]. Вместе с тем ошибочно полагать, что данное разъяснение не может иметь исключений. На наш взгляд, *несмотря на положения п. 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 Уголовного кодекса Российской Федерации» некоторым образом нивелировало значимость официальных рекомендаций Пленума Верховного Суда РФ о квалификации специаль-

---

[1] Заседание Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. [Электронный ресурс] // URL: http://www.vsrf.ru/press_center/news/26093 (дата обращения: 06.12.2017).

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

ных 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[1]. После апрельских изменений отечественного уголовного закона правоприменитель опять оказался в ситуации частичной неопределенности 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 кражу[2].

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.

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

---

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

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

с банковского счета в размере 33 864 рубля, чем причинил потерпевшей значительный материальный ущерб[1].

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»[2]. 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.

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 рублей, принадлежащих потерпевшему[3].

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

---

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

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

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

 *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: 591,06 рубля, 354 рубля, 970,82 рубля. Примерно в это же время, находясь уже в другом магазине, дважды осуществило оплату приобретенного товара банковской картой потерпевшего на суммы: 151,80 рубля, 105 рублей*[1].

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 может основываться на 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).

 *Осуществляя переквалификацию с п. «г» ч. 3 ст. 158 УК РФ на ст. 159.3 УК РФ, суд, ссылаясь на указанное выше разъяснение*

---

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

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 PayPass, 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].

Вместе с тем современная редакция ст. 159.3 УК РФ, с учетом дополнения ч. 3 ст. 158 и ч. 3 ст. 159.6 УК РФ новым квалифицирующим признаком – «хищение с банковского счета, а равно в отношении электронных денежных средств» – позволяет предложить и другой подход разрешения конкуренции уголовно-правовых норм об ответственности за хищения с банковского счета потерпевшего, а равно в отношении электронных денежных средств. В соответствии с п. 19 ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» под электронным средством платежа понимается средство и (или) способ, позволяющие 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. Объективная сторона преступления, предусмотренного п. «в» ч. 3 ст. 159.6 УК РФ, подразумевает

---

[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.

распоряжение денежными средствами, зачисленными на банковский счет, и электронными денежными средствами путем неправомерного манипулирования компьютерной информацией и вмешательства в функционирование средств ее хранения, обработки и передачи, что возможно исключительно с использованием электронных средств платежа, к которым относятся системы дистанционного банковского обслуживания (далее – ДБО), электронные кошельки, банкоматы, платежные шлюзы, банковские и предоплаченные платежные карты и т. п. По существу, данный вид хищения, совершенный с банковского счета, а равно в отношении электронных денежных средств, с точки зрения законодателя можно было бы рассматривать как квалифицированное мошенничество с использованием электронного средства платежа, где квалифицирующим признаком является совершение деяния путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Законодатель исключил из объективной стороны преступления, предусмотренного ст. 159.3 УК РФ, обязательные действия, направленные на обман работника кредитной, торговой или иной организации, и, напротив, дополнил ее действиями, связанными с применением технологий безналичных расчетов, то есть, по сути, описал отличный от ст. 159 УК РФ способ совершения данного вида мошенничества, что позволяет распространить на ст. 159.3 УК РФ подход, ранее примененный к преступлению, предусмотренному ст. 159.6 УК РФ, и рассматривать хищение с применением электронного средства платежа как специальный вид мошенничества с отличным от классического способом совершения.

Таким образом, действия виновного лица, прямо или косвенно сопряженные с использованием электронных средств платежа, в зависимости от их объема и умысла на достижение конкретных преступных результатов могут быть квалифицированы по ст. 159, по ст. 159.3 или по п. «в» ч. 3 ст. 159.6 УК РФ.

Так, в случае создания мошенниками поддельных сайтов, внешне похожих на веб-ресурсы кредитных организаций, либо платежных шлюзов, рассылки ими электронных писем или *SMS*, содержащих ложную информацию, а также использования телефонной связи, в том числе *IP*-телефонии, для обмана потерпевших или введения их в заблуждение, в результате чего они самостоятельно, используя

электронные средства платежа, перечисляют денежные средства мошеннику, действия виновного квалифицируются по ст. 159 УК РФ.

При других обстоятельствах схожие действия являются приготовлением к совершению преступления, предусмотренного ст. 159.3 УК РФ. Отличие состоит в том, что в результате обмана и введения в заблуждение потерпевших, последние сообщают мошенникам реквизиты доступа к электронным средствам платежа, позволяющие распоряжаться их денежными средствами на банковских счетах либо электронными денежными средствами. Классификация электронных средств платежа весьма широка, соответственно, и сведения, которыми завладевают мошенники с целью дальнейшего хищения, разнообразны. Например, это могут быть имя пользователя и пароль для подключения к системе ДБО либо код, присылаемый в *SMS* для подтверждения транзакции, или реквизиты банковской карты, включая код безопасности (*CVV*), позволяющие оплачивать покупки и услуги с помощью платежных шлюзов в сети Интернет. Разумеется, мошенники не обязательно собирают такие сведения своими силами. На стадии приготовления к совершению преступления они могут приобрести их у других лиц, преступная специализация которых состоит именно в собирании конфиденциальной информации, в том числе охраняемой законом.

Помимо перечисленных выше сведений, на теневых рынках киберкриминальной направленности активно предлагаются цифровые копии (дампы) банковских карт и персональные идентификационные номера (ПИН-коды) к ним либо уже готовые к использованию поддельные банковские карты, предоставляющие доступ к распоряжению банковскими счетами потерпевших. Здесь представляется необходимым отметить, что действия, направленные на собирание сведений, составляющих банковскую тайну, любым незаконным способом, содержат признаки преступления, предусмотренного ст. 183 УК РФ, а изготовление и сбыт поддельных платежных карт – преступления, предусмотренного ст. 187 УК РФ.

Что касается реализации объективной стороны преступного посягательства, если мы рассматриваем его как специальный вид мошенничества, предусматривающий особый способ его совершения, любые действия с использованием поддельных либо украденных платежных карт охватываются диспозицией ст. 159.3 УК РФ, если они направлены на хищение денежных средств с банковских счетов потерпевших или в отношении электронных денежных средств, неза-

висимо от того, были ли они предъявлены работнику какой-либо организации либо вводились для считывания в банкомат или платежный терминал, равно как действия, связанные с использованием реквизитов потерпевших для подключения к системам интернет-банкинга, мобильного банка, электронных кошельков, платежных шлюзов и т. п., то есть с использованием электронных средств платежа без признаков деструктивного вмешательства в их функционирование.

И наконец, способом совершения преступления, предусмотренного п. «в» ч. 3 ст. 159.6 УК РФ, помимо использования электронных средств платежа для осуществления безналичных расчетов либо операций с электронными денежными средствами, являются обязательные действия, содержащие ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, что требует от мошенников обладания специальными техническими знаниями и приискания орудий совершения преступления, в качестве которых используются вредоносные программы, значительно усиливающие возможности преступников. Этот способ охватывает воздействие на функционирование вычислительных устройств, управляющих работой банкоматов, и личных компьютеров пользователей, с которых осуществляется доступ к интернет-банкингу или электронным кошелькам, и смартфонов, подключенных к сервису мобильного информирования, и автоматизированных банковских систем и т. д., в результате которого мошенники совершают хищение с банковского счета либо в отношении электронных денежных средств. Очевидно, что реализация объективной стороны преступления, предусмотренного ст. 159.6 УК РФ, в рассмотренных выше случаях сама по себе осуществляется посредством получения неправомерного доступа к электронному средству платежа потерпевшего, используя который преступник совершает хищение денежных средств с банковского счета потерпевшего либо в отношении его электронных денежных средств. В связи с этим полагаем, что введение в ч. 3 ст. 159.6 УК РФ нового квалифицирующего признака является избыточным уточнением.

Таким образом, составы рассмотренных преступлений, предусмотренных ст.ст. 159, 159.3, 159.6 ч. 3 п. «в» УК РФ, объединяет:

1. Списание денежных средств с банковского счета или электронных денежных средств из соответствующего реестра (за исключением вмешательства преступников в функционирование электронных банковских систем, не связанных напрямую с обслуживанием расчетных счетов).

2. Использование электронных средств платежа.

3. Тайное совершение хищения (за исключением состава преступления, предусмотренного ст. 159 УК РФ, то есть случаев, когда потерпевший самостоятельно перечисляет денежные средства мошенникам).

Вместе с тем, несмотря на то, что такой подход к разрешению конкуренции уголовно-правовых норм об ответственности за хищения с банковского счета потерпевшего, а равно в отношении электронных денежных средств представляется логичным и обоснованным и как минимум требующим дополнительного осмысления, очевидно, что законодатель, принимая указанные изменения и дополнения в уголовный закон, не руководствовался этими соображениями. Подтверждением этого вывода является тот факт, что помимо ч. 3 ст. 159.6 УК РФ, новый квалифицирующий признак – совершение хищения «с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ)» – введен и в п. «г» ч. 3 ст. 158 УК РФ. Обоснованность этой новеллы вызывает сомнения в кругу технических специалистов, поскольку, как отмечалось выше, хищение с использованием электронного средства платежа охватывается ст. 159.3 УК РФ, при том что классический способ совершения мошенничества – путем обмана и введения в заблуждение – в диспозиции этой статьи теперь отсутствует, как и в другой статье – 159.6 УК РФ, предусматривающей специальный вид мошенничества – в сфере компьютерной информации. Если, как обосновано выше, любое хищение с использованием электронного средства платежа в связи с модификацией ст. 159.3 УК РФ рассматривается как специальный вид мошенничества, непонятно, какие действия могут содержать признаки деяния, предусмотренного п. «г» ч. 3 ст. 158 УК РФ?

В связи с этим представляется полезным в динамике рассмотреть отдельные действия злоумышленников, охватываемые единым замыслом, с точки зрения их возможной уголовно-правовой квалификации, начиная с момента возникновения преступного умысла на мошенничество в сфере компьютерной информации, продолжая при-

готовлением к совершению преступления и заканчивая реализацией преступных планов.

После возникновения преступного умысла, на стадии приготовления к хищению в сфере компьютерной информации, злоумышленники приискивают орудия совершения преступления, в качестве которых выступают вредоносные программы. В зависимости от целей использования вредоносные программы могут быть разработаны самими соучастниками, планирующими хищение, если позволяет их технический уровень, либо приобретены у иных лиц. В любом случае такие действия содержат признаки преступления, предусмотренного ст. 273 либо ч. 1 ст. 274.1 УК РФ.

Дальнейшие действия направлены на получение неправомерного доступа к компьютерным системам и пользовательской информации, чтобы путем вмешательства в их функционирование собрать сведения, содержащие персональные данные потерпевших и реквизиты используемых ими электронных средств платежа, либо непосредственно осуществить хищение с их банковского счета или в отношении электронных денежных средств. Получение неправомерного доступа к компьютерной информации квалифицируется по ст. 272 или ч. 2 ст. 274.1 УК РФ. Соответственно, незаконное получение сведений, содержащих банковскую тайну, охватывается ст. 183 УК РФ.

И наконец, в процессе доведения преступного умысла до конца злоумышленники, получив с использованием вредоносных программ несанкционированный доступ к электронному средству платежа, совершают хищение путем ввода, удаления, модификации компьютерной информации с целью составления и передачи распоряжения на перевод денежных средств. После успешного списания денежных средств злоумышленники, используя возможности вредоносных программ, могут совершить действия, направленные на сокрытие следов преступления путем удаления и блокирования компьютерной информации. Оконченное преступление квалифицируется по ст. 159.6 УК РФ.

Если же хищение совершается с помощью электронных средств платежа путем использования незаконно полученных реквизитов доступа к ним, деяние содержит признаки состава преступления, предусмотренного ст. 159.3 УК РФ.

Таким образом, главной целью злоумышленников по составам ст.ст. 159.3, 159.6 УК РФ является получение неправомерного доступа к электронным средствам платежа. Отличительным признаком является то, что в случае ст. 159.3 УК РФ злоумышленником не оказывается воздействие на компьютерную систему, а в случае ст. 159.6 УК РФ такое

воздействие оказывается. Также необходимо отметить, что технически осуществить хищение с банковского счета без использования электронного средства платежа невозможно. Теоретически можно использовать реквизиты банковской карты при оплате товаров в сети Интернет – это могло бы квалифицироваться по п. «г» ч. 3 ст. 158 УК РФ, однако и в этом случае для списания денежных средств с банковского счета технически используется электронное средство платежа.

Необходимо отметить, что постановлением Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» разъяснено, что «действия лица следует квалифицировать по статье 159.3 УК РФ в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой. При этом не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата без участия уполномоченного работника кредитной организации. В этом случае содеянное следует квалифицировать как кражу». Однако данные разъяснения даны относительно старых редакций ст.ст. 158 и 159.3 УК РФ. В связи с этим их применение для разрешения настоящей конкуренции уголовно-правовых норм представляется не вполне правильным.

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.)[1]. При этом в обоснование собственного подхода автор отдельно оговаривает, что основное отличие кражи от мошенничества с использованием электронных средств платежа за-

[1] 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.

ключается именно в способе хищения. Для квалификации деяния как мошенничества с использованием электронного средства платежа необходимо целенаправленное воздействие на ПО, приложение, устройство, позволяющее получить неправомерный доступ к счету владельца[1].

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

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 на память терминала: ПО, 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 ПО, позволяющего подтвердить принятие денежной купюры в устрой-

---

[1] Там же.

стве, 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 рублей со специального счета терминала по приему платежей от населения на счет 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 (атаками с помощью BlackBox, при которых лицо просверливает отверстие в банкомате, подключается через USB-порт и использует вредоносное ПО, чтобы дать команду на выдачу денежных средств). Здесь 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 ПО банкомата. При этом следует, конечно же, оговориться, что 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.

Н. была осуждена по ч. 2 ст. 159 УК РФ. В соответствии с приговором суда, Н., имея умысел на хищение чужого имущества,

---

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

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 рублей, после чего распорядилась ее деньгами по своему усмотрению, причинив Ш. значительный материальный ущерб на общую сумму 15 500 рублей[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

---

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

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-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.*

[1] Потапкин С. Н., Солдатов А. В., Утешева Т. Т. Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике // Библиотека научных публикаций Электронного юридического справочника системы «Гарант». № 1 (5). 2015. С. 3.

[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 3. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

3.1. Орудия и средства совершения преступлений

Преступные посягательства данной категории совершаются в сфере обработки, передачи, хранения компьютерной информации, следовательно, средствами преступлений являются непосредственно компьютерные устройства, их сети и установленное на них ПО.

Средства совершения преступлений:

– программное обеспечение;
– компьютерные устройства;
– компьютерные сети.

Подавляющее количество преступлений в сфере компьютерной информации совершается с помощью вредоносного ПО. В этом случае орудием совершения преступления выступает вредоносная программа, значительно усиливающая возможности преступника.

В качестве орудия совершения преступления может быть использована и легальная программа, функциональность которой предоставляет преступникам возможность достижения своих целей.

Орудия совершения преступлений:

– легальное ПО, стандартные функциональные возможности которого представляют потенциальную опасность;
– вредоносное ПО, то есть специально созданные программы либо модифицированное легальное программное обеспечение.

Например, распространено использование программ для удаленного управления компьютерами с целью осуществления неправомерного доступа и программ, шифрующих пользовательские данные с целью требования передачи денежных средств за восстановление информации.

Большинство легальных программ, используемых преступниками в противоправной деятельности, предназначены для удаленного несанкционированного доступа к компьютеру, управления системой и ее администрирования. Выбор конкретного приложения обусловлен задачами, которые решаются на том или ином этапе совершения преступного посягательства.

Легальные программы удаленного доступа определяются антивирусным ПО как условно опасные и детектируются, если пользователь включил опцию информирования об их обнаружении. Классифика-

ция детектируемых объектов «Лаборатории Касперского» относит такие программы к классу *RiskWare* и определяет с именем *RemoteAdmin*. Популярность этих программ среди преступников обусловлена тем, что при наличии широких возможностей, обеспечиваемых штатной функциональностью, их применение позволяет ослабить бдительность пользователей.

Во-первых, такие программы, как было сказано выше, определяются антивирусным ПО с менее критичным именем как условно опасные, в связи с чем пользователи не видят в них особой угрозы.

Во-вторых, многие из этих программ являются доверенными программами пользователя, установлены с его ведома и не вызывают у него подозрений.

В-третьих, большинство используемых легальных программ являются лицензионными, они постоянно совершенствуются разработчиком и поэтому не требуют дополнительных средств на их доработку.

В-четвертых, легальные программы обладают функциональными возможностями, достаточными для достижения преступных целей и, как правило, не требуют какой-либо дополнительной модификации за исключением некоторых случаев, например когда необходимо отключить оповещение пользователя о работе программы либо ее модулей.

Из весьма большого количества можно выделить четыре легальные программы, которые активно используются для несанкционированного удаленного управления, контроля и администрирования: *RMS, Ammyy Admin, TeamViewer* и *LiteManager*.

В определенных случаях эти программы подвергаются менее или более значительной модификации, которая может привести к изменению их поведения (набора действий) в системе, которое будет соответствовать другому классу детектируемых объектов – *Malware* (категории вредоносных программ). Тем не менее, преступники прилагают все усилия и ухищрения, чтобы используемые ими программы воспринимались как условно-опасные и подпадали под класс *RiskWare*, что предоставляет им дополнительные преимущества.

Один из таких способов реализуется с помощью технологии *DLL Hijacking*, эксплуатирующей особенности функционирования ОС *Windows*. Способ заключается в помещении в одну папку с файлом программы удаленного управления вредоносного библиотечного файла (*dll*-библиотеки), причем с таким же именем, что и расположенная в другой директории легальная библиотека. При запуске про-

грамма вместо легальной библиотеки загружает вредоносную, которая размещена «ближе». Например, для сокрытия от пользователя отображаемых на экране графических признаков работы программы *TeamViewer* (значка, окна сообщений) преступники осуществляют подмену библиотеки *msvfw32.dll*.

Помимо программных средств, в более редких случаях в качестве орудия совершения преступления используется аппаратно-программный комплекс, который может быть достаточно простым, например устройство, скрыто устанавливающееся в разрыв интерфейса клавиатуры для перехвата нажатия клавиш, так и более сложным. Нередко аппаратно-программные комплексы используются преступниками при хищении денежных средств из банкоматов, некоторые из таких комплексов, помимо аппаратной и программной, имеют электромеханическую часть.

3.2. Вредоносные программы и их подвиды

Определение вредоносной программы с уголовно-правовой точки зрения содержится в диспозиции ст. 273 УК РФ.

Вредоносная программа — это компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации

Признаки состава данного преступления, по существу, можно рассматривать как признаки, позволяющие признать конкретную компьютерную программу вредоносной.

Признаками вредоносного ПО, которые могут быть частично установлены в ходе судебной компьютерной экспертизы, являются:

– обладание функциональностью уничтожения, блокирования, модификации, копирования пользовательской информации или нейтрализации средств защиты компьютерной информации;

– установление без явного одобрения пользователем;

– работа скрыто от пользователя;

– производство операции с информацией, не санкционированной пользователем явно.

Однако вопрос «Является ли программа вредоносной?» перед судебным экспертом некорректен, поскольку ответ на вопрос выходит за пределы профессиональной компетенции эксперта.

Признание программы вредоносной является исключительной прерогативой следователя и суда, поскольку помимо технических необходимо установить наличие признаков правового плана:

– прямой умысел на этапе разработки программы, доподлинное и безусловное осознание предназначения создаваемой программы – «заведомо предназначенная»;

– субъективное восприятие потерпевшим наличия угрозы от компьютерной программы.

Вследствие большого разнообразия вредоносных программ, для их классифицирования применяют различные основания. Самая общая классификация, широко применяемая в настоящее время, выделяет из класса вредоносных программ (*Malware*) следующие подклассы: программы-вирусы (*Virus*), программы-черви (*Worm*) и троянские программы (*Trojan*).

Классификация вредоносных программ:

– вирусы (*Viruses*): обладают способностью к саморазмножению и распространению по локальным ресурсам компьютера;

– черви (*Worms*): обладают способностью к саморазмножению и распространению по компьютерным сетям;

– троянские программы (*Trojan programs*): не умеют создавать свои копии и неспособны к самовоспроизведению.

К первым двум подклассам программ относятся вирусы и черви, которые без ведома пользователя саморазмножаются на компьютерах и в компьютерных сетях, при этом каждая последующая копия также обладает способностью к саморазмножению.

В некоторых последних вредоносных кампаниях было зафиксировано использование вредоносных программ такого подкласса. Например, в мае 2017 г. была осуществлена наиболее масштабная за обозримое время атака с применением программы-шифровальщика *WannaCry*. Только за один день вредоносная программа атаковала компьютеры пользователей более чем в 74 странах. Наибольшее количество заражений было зафиксировано в России, серьезно пострадали и другие страны, в первую очередь – Украина, Индия, Тайвань. По своему основному предназначению *WannaCry* имеет те же функциональные возможности, что и другие шифровальщики, – модификация пользовательских данных на компьютере и последующее требование выкупа за их восстановление, но столь массовые случаи заражения были связаны со способом распространения.

Первичное заражение осуществлялось посредством эксплуатации уязвимости ОС *Windows*. После успешного проникновения хотя бы на один компьютер, подключенный к локальной сети, шифровальщик *WannaCry* распространялся по сети на другие устройства как червь (*Worm*). По этой причине наибольший ущерб от шифровальщика *WannaCry* был причинен организациям, имеющим крупные корпоративные компьютерные сети.

Рис. 3.1. Сообщение шифровальщика *WannaCry*

Приведено сообщение, выводимое программой-шифровальщиком *WannaCry* на экран компьютера пользователя, содержащее требование выкупа за восстановление модифицированных программой данных (*рис. 3.1*).

Программы другого вида, относящиеся к третьему подклассу – троянские программы (*Trojan programs*), – не умеют создавать свои копии и не способны к самовоспроизведению. В этом случае распространение копий по сети и заражение удаленных компьютеров происходит по команде с сервера управления.

Другая классификация вредоносных программ учитывает такую их функциональную особенность, как возможность автономной работы.

Классификация вредоносных программ:

– автоматические: предназначены для автономной работы, самостоятельно инициируют сетевые соединения с удаленными серверами при необходимости передачи информации;

– полуавтоматические: обладают способностью работать автономно, инициировать сетевое взаимодействие с удаленными серверами, но также наделены функцией исполнения передаваемых им команд;

– ручные: работают в соответствии с поступающими командами.

Автоматические вредоносные программы не нуждаются во внешнем управлении, заложенные в них функциональные возможности реализуются в автономном режиме. При необходимости передать информацию с зараженного компьютера на удаленный сервер программа самостоятельно инициирует соединение. Например, программа-шифровальщик (*Trojan-Ransom*) после кодирования пользовательских данных инициирует сетевое соединение с удаленным сервером и передает на него информацию, содержащую идентификатор зараженного компьютера для последующего восстановления пользовательских данных в случае выплаты денежных средств.

Полуавтоматические программы также способны работать автономно, реализуя свое предназначение, инициировать соединение с удаленным сервером для передачи информации, но также имеют возможность получать с сервера управления команды и выполнять их. К полуавтоматическим относятся практически все троянские программы, предназначенные для хищения в электронных платежных системах (*Trojan-Banker*). Например, попав в систему, они самостоятельно сканируют пользовательскую информацию, находят следы использования программ-клиентов ДБО, платежные документы, учетные записи и пароли и т. п. и передают собранную информацию на сервер управления. Но при этом они обладают возможностью получения внешних команд от сервера на загрузку дополнительных программных модулей либо совершение несанкционированной финансовой операции.

Вредоносные программы, работающие в ручном режиме, предназначены для управления с помощью внешних команд. Такими программами могут быть троянские программы для удаленного управления компьютером (*Trojan-Backdoor*) либо программы, предназначенные для управления диспенсером банкомата с использованием штатной клавиатуры (ПИН-пада). Подробнее о возможностях таких программ будет рассказано ниже.

3.3. Классификация троянских программ

Основным признаком, который служит для дифференцирования троянских программ, является вид действия (поведение), которое они выполняют на компьютере. Наиболее распространенные в настоящее время виды троянских программ приведены в списке ниже (согласно классификации детектируемых антивирусным ПО Лаборатории Касперского объектов).

Классификация троянских программ:

– программа-шпион (*Trojan-Spy*): ведение электронного шпионажа за пользователем, в том числе перехват вводимых с клавиатуры данных, изображений экрана, списка активных приложений;

– программа-банкер (*Trojan-Banker*): кража пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам;

– программа-шифровальщик (*Trojan-Ransom*): модификация пользовательских данных на компьютере либо блокировка работы компьютера с целью получения выкупа за восстановления доступа к информации;

– программа для удаленного управления (*Trojan-Backdoor*): скрытое удаленное управление компьютером и полный доступ к пользовательской информации;

– программа-загрузчик (*Trojan-Downloader*, *Trojan-Dropper*): загрузка и установка на компьютер вредоносных программ и их новых версий;

– программа для эксплуатации программных уязвимостей (*Exploit*): скрытая эксплуатация уязвимостей ПО пользователя.

Большинство современных троянских программ сочетают в себе не одно поведение, а целый набор видов деятельности, предоставляющий преступникам самые широкие возможности для манипулирования пользовательской информацией. Например, программа-банкер, определяемая антивирусным ПО «Лаборатории Касперского» с именем *Trojan-Banker.Win32.RTM,* помимо присущей только этому виду троянских программ функциональности поиска и копирования пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам, обладает и многими другими возможностями – поиска файлов по именам, записи истории

нажатий клавиш клавиатуры, записи видео и создании снимков экрана, копирования буфера обмена, блокирования и нарушения работы ОС, получения от сервера управления команд на запуск дополнительных программных модулей, отправки собранной информации на сервер управления и т. п.

Изначально под троянской программой понималась разновидность вредоносной программы, которая устанавливалась в компьютерную систему под видом легального ПО и работала маскируясь под него. В настоящее время смысл в такой трактовке утрачен. Напротив, преступники пытаются максимально скрыть от пользователя загрузку, установку и работу вредоносной программы, используя для этого различные способы и средства, о которых будет сказано ниже.

Троянские программы не обладают функциональными возможностями самостоятельного воспроизведения и распространения. Для загрузки троянских программ в компьютерную систему без ведома пользователя применяют различные способы.

Способы проникновения в систему:

– рассылка электронных писем, содержащих вредоносное вложение;

– применение связок эксплойтов при веб-серфинге пользователей в сети Интернет;

– внедрение вредоносного кода в распространяемое легальное ПО;

– распространение в локальной сети посредством применения штатных программных средств;

– физический доступ к целевой системе.

Для проникновения в систему с помощью сообщений электронной почты преступники осуществляют целевую либо массированную спам-рассылку писем, содержащих в качестве вложения специальным образом сформированный документ. Открытие пользователем данного документа приводит к скрытой загрузке вредоносной программы и установке ее в систему.

В другом варианте вредоносное письмо содержит не вложение, а ссылку на внешние интернет-ресурсы, при переходе по которой компьютер пользователя подвергается атаке набором эксплойтов. При успешном срабатывании одного из эксплойтов на компьютер пользователя загружается вредоносное ПО. При необходимости, когда возможности совершения несанкционированных действий на

компьютере пользователя ограничены правами его учетной записи, преступниками может быть применен локальный эксплойт для повышения привилегий.

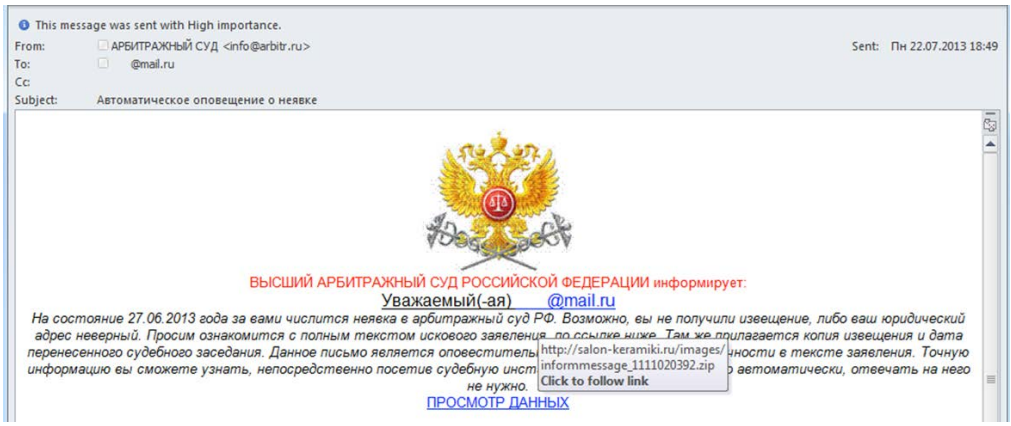


Рис. 3.2. Пример нежелательного письма

Для заражения компьютеров преступники осуществляют рассылку вредоносных писем от имени государственных органов, чтобы пользователь относился к их содержанию с доверием (*рис. 3.2*). Однако при наведении курсора на ссылку, содержащуюся в сообщении, отображается сторонний адрес, никоим образом не ассоциированный с именем отправителя (*http://salon-keramiki.ru/images/informmessage_1111020392.zip)*. В случае если пользователь, введенный в заблуждение текстом письма, перейдет по ссылке, на его компьютер загрузится вредоносный файл.

Для заражения компьютеров может быть использован так называемый метод *drive-by*-загрузки, когда в процессе перемещения пользователя по сайтам в сети Интернет его компьютер скрыто перенаправляется с легитимной, но скомпрометированной страницы на криминальный ресурс, где подвергается атаке набором эксплойтов (*рис. 3.3*).

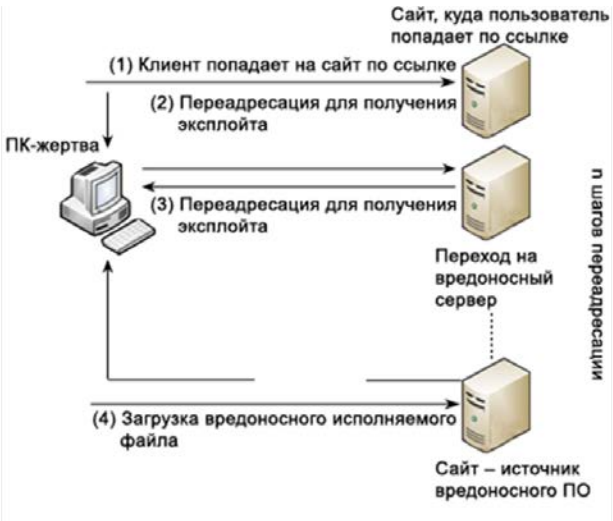


Рис. 3.3. Схема атаки набором эксплойтов

Описанные первые два способа наиболее распространены и хорошо известны. В более редких случаях преступники предварительно получают несанкционированный доступ к сетевым ресурсам разработчика легальных программ, после чего внедряют в распространяемое им ПО свой вредоносный код. Известный случай – распространение вредоносной программы троянской программы-банкера *Lurk* установщиком программы удаленного администрирования *Ammyy Admin*.

При наличии у преступников доступа хотя бы к одному компьютерному устройству локальной сети организации дальнейшее распространение вредоносных программ на другие компьютеры и серверы может осуществляться с помощью штатных программных средств и протоколов. Например, неоднократно фиксировалось использование программы *PsExec* от корпорации *Microsoft* для автоматизированного развертывания вредоносного ПО на всех компьютерах, входящих в корпоративную сеть.

Физический доступ к компьютерной системе может быть обеспечен вовлечением в преступление работника потерпевшей организации либо проникновением преступников за охраняемый периметр. В этом случае загрузка вредоносной программы в систему осуществляется посредством подключения к ней внешнего электронного носителя информации.

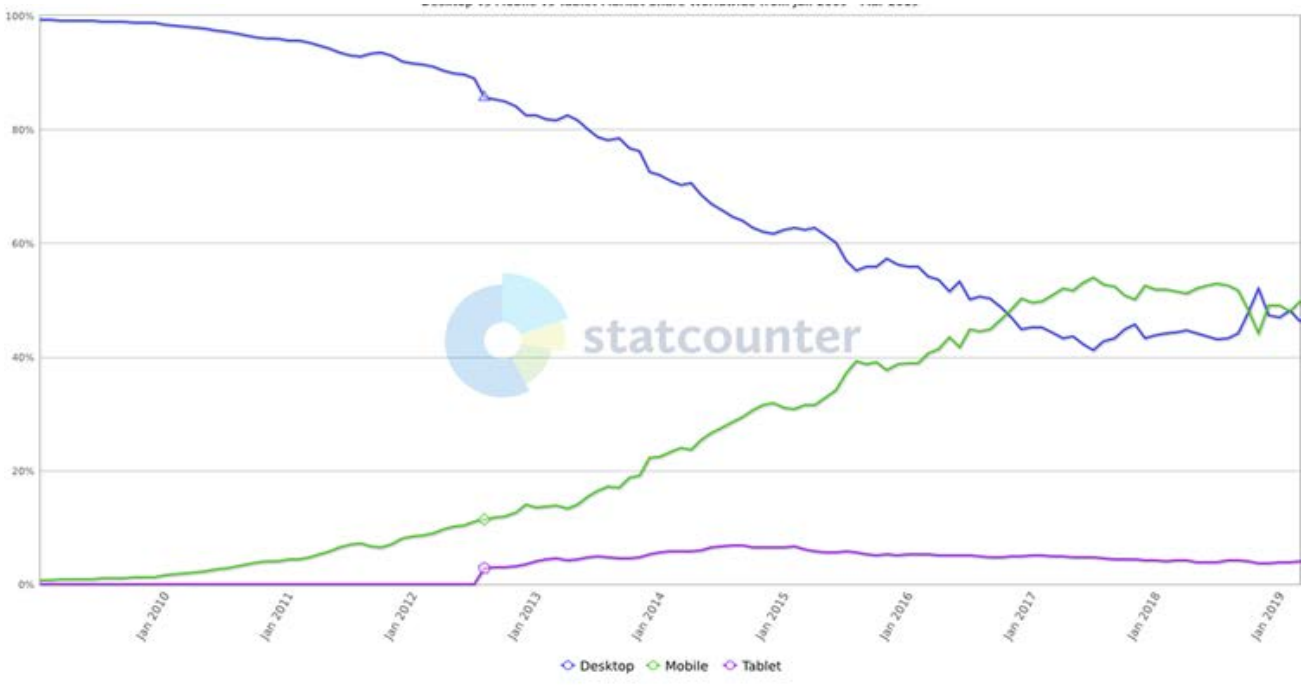


Рис. 3.4. Распределение интернет-трафика по видам устройств[1]

[1] Согласно данным ресурса *StatCounter*.

Отдельного упоминания заслуживает постоянно усугубляющаяся ситуация с распространением троянских программ для мобильных устройств, в первую очередь, под управлением ОС *Android*. Это обусловлено как ростом количества пользователей мобильных устройств (*рис. 3.4*), так и технологическим совершенствованием их элементной базы и сетей передачи данных, что позволяет активно развивать новые мобильные сервисы, использующие электронные средства платежа.

Такое положение дел привело к всплеску распространения мобильного вредоносного ПО, реализующего функциональные возможности троянских программ – шпионов (*Trojan-Spy*) и банкеров (*Trojan-Banker*):

– перехват, удаление или модификация входящих и исходящих *SMS*, рассылка *SMS* (правила перехвата предусмотрены заранее или в режиме реального времени модифицируются оператором вредоносного ПО);

– удаленный рабочий стол, позволяющий дистанционно управлять мобильным устройством;

– запись разговоров, звуков или изображений со встроенной камеры;

– отправка *USSD*-команд для получения информации о подключенных банковских картах, их балансе, осуществления быстрых переводов;

– использование эксплойтов для получения максимальных привилегий для сокрытия приложения, предотвращения его удаления, удаления или деактивации антивирусов, копирования данных других приложений;

– установка других модулей вредоносного ПО.

Перечисленные функциональные возможности вредоносных мобильных приложений позволяют осуществлять дистанционные способы хищения путем:

– непосредственного взаимодействия с сервисами ДБО и перевода денежных средств на сторонние счета;

– получения сведений о реквизитах банковской карты и дальнейшего запроса денежных средств либо оплаты товаров и услуг через сторонние сервисы (переводы с карты на карту, интернет-торговля).

Основными способами распространения мобильного вредоносного ПО являются:

– социальная инженерия – склонение пользователя самостоятельно произвести установку ПО под каким-либо предлогом (переход по ссылке, *SMS*-спам, маскировка под легальное приложение в официальных магазинах);

– эксплуатация уязвимостей – установка с использованием уязвимости в имеющемся ПО (веб-браузер, мессенджер и т. д.);

Кроме того, в мобильных ОС существуют уязвимости, позволяющие произвести установку вредоносного ПО при подключении устройства к компьютеру с помощью кабеля, например для синхронизации пользовательских данных.

3.4. Программно-аппаратные устройства

В широком смысле обычный компьютер с установленным на него ПО уже является программно-аппаратным устройством, но в данном случае под ним необходимо понимать специально созданное в преступных целях устройство и программы к нему.

Программно-аппаратные устройства не получили такого распространения при совершении преступлений в сфере компьютерной информации как вредоносные программы. Это обусловлено несколькими факторами. Разработка устройства – более затратное по времени и средствам мероприятие, чем создание компьютерной программы, если, конечно, иметь в виду примерно сравнимый уровень сложности. В отличие от программы, воспроизведение копий любого устройства требует определенных мощностей, пусть даже кустарных, и комплектующих. При использовании аппаратно-программного устройства невозможно обеспечить такой же высокий уровень конспирации, как в случае применения вредоносных программ. Установленные на сетевые кабели либо подключенные к компьютерам устройства для несанкционированного перехвата и записи данных могут быть легко обнаружены при визуальном осмотре.

Тем не менее при определенных способах совершения преступных посягательств разработка и использование аппаратно-программного устройства может принести значительный преступных доход. Многие такие разработки достаточно уникальны, поскольку создаются для решения конкретных задач. Другие получили определенное признание в криминальной среде и, соответственно, распространение при совершении преступлений.

Наиболее простые аппаратные решения, используемые как орудия компьютерных преступлений, – это устройства для записи действий пользователя в компьютерной системе. Они могут быть подключены как обычный *USB*-флеш-накопитель либо в целях конспирации внедрены внутрь корпуса. Менее сложное устройство – аппаратный кейлогер – просто включается в разрыв кабеля, соединяющего клавиатуру с системным блоком компьютера, и используется для регистрации и записи нажатий клавиш (*рис. 3.5*). К этому же перечню можно отнести и устройства для перехвата данных по компьютерным сетям, устанавливаемые в разрыв либо параллельно на сетевые кабели.

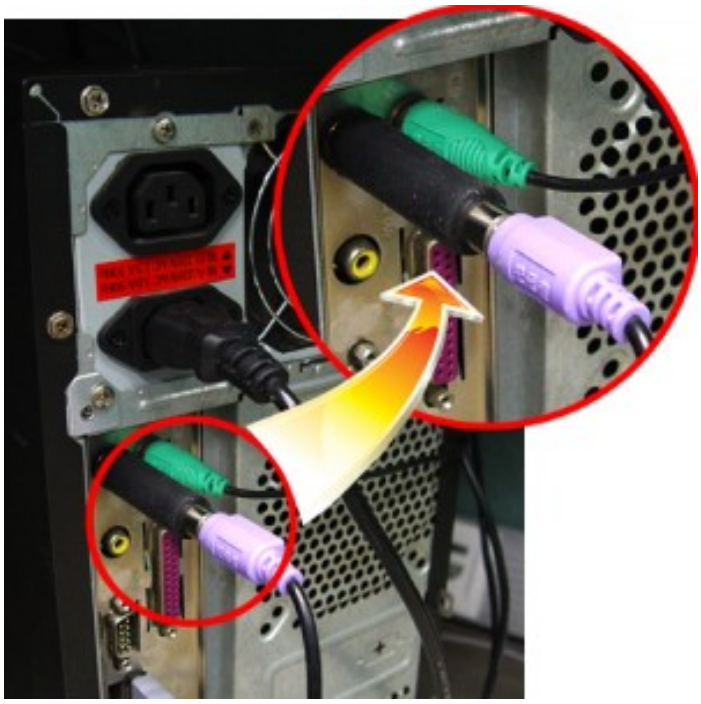


Рис. 3.5. Аппаратный кейлогер

К более сложным техническим решениям, разработанным для совершения преступлений, применимо иное название – аппаратно-программные комплексы. К аппаратно-программным комплексам относятся так называемые бот-фермы, то есть компьютерные системы, эмулирующие работу большого количества устройств с отдельными каналами подключения к сети Интернет. Такие системы используются для массовых кампаний распространения вредоносного ПО на мобильные устройства под управлением ОС *Android* посредством *SMS*-рассылки либо для осуществления *DDoS*-атак.

Весьма существенную угрозу для банковской сферы представляют аппаратно-программные комплексы, разработанные для совершения хищений денежных средств из банкоматов, – так называемые *Black Box*. Такой комплекс является, по сути, мини-компьютером

с установленным на него специальным ПО, который подключают к диспенсеру (механизму выдачи денег) вместо штатного компьютера, расположенного в сервисной зоне банкомата (*рис. 3.6*). После этого управление банкоматом может осуществляться с помощью технологий беспроводной передачи данных, например со смартфона, либо с использованием кабеля, подключенного к диспенсеру через специально просверленное в корпусе банкомата отверстие.

Рис. 3.6. Установка аппаратно-программного комплекса *Black Box* в корпус банкомата

3.5. Отдельные виды компьютерных преступлений

По сути, большинство преступлений могут быть совершены посредством несанкционированного доступа к компьютерной информации и манипулирования ею и (или) с использованием компьютерных программ и средств компьютерной техники. В этом случае объектом преступного посягательства выступают общественные отношения, охраняемые конкретной статьей Уголовного кодекса, а использование информационно-коммуникационных технологий, компьютерных устройств и их сетей, а также вредоносных программ необходимо рассматривать как способ, средства и орудия совершения преступления соответственно. Как правило, такие общественно опасные деяния

совершаются из корыстной заинтересованности в ее широком понимании (например, из недобросовестной конкуренции). При этом наиболее прямой путь к преступному обогащению, реализующий несанкционированный доступ к компьютерным данным, – совершение хищений в электронных платежных системах, в первую очередь, системах дистанционного банковского обслуживания (ДБО). Однако возможны и другие мотивы (хулиганские побуждения, кибертерроризм, создание общественного резонанса в иных преступных целях и т. п.).

Обобщив закономерности развития совершаемых за последние годы преступлений в сфере компьютерной информации, можно выделить наиболее распространенные их виды:

– хищения в электронных платежных системах;

– модификация компьютерных данных с требованием передачи денежных средств за восстановление информации;

– осуществление *DDoS*-атак в рамках недобросовестной конкуренции либо с целью получения денежных средств за их прекращение;

– модификация компьютерных данных либо осуществление DDoS-атаки из хулиганских побуждений;

– кибертерроризм.

В свою очередь, наиболее распространенные преступления в электронных платежных системах можно обобщить следующим образом:

– хищения, связанные с получением неправомерного доступа к сетевой инфраструктуре финансово-кредитных организаций;

– хищения, связанные с получением неправомерного доступа к сетевой инфраструктуре юридических лиц – клиентов ДБО;

– хищения, связанные с получением неправомерного доступа к компьютерам физических лиц – клиентов ДБО.

Вместе с тем нельзя обойти вниманием все более возрастающую тенденцию в применении компьютерных и сетевых технологий как средств совершения преступлений, объектом которых выступают любые общественные отношения, а не только отношения в сфере компьютерной информации. Данный факт находит свое отражение и в том, что эксперты в области информационной безопасности все чаще привлекаются в качестве специалистов при проведении следственных действий и оперативно-разыскных мероприятий по преступлениям

традиционной направленности: убийствам, мошенничеству, незаконным организации и проведению азартных игр и т. п.

Для лучшего понимания, как преступники используют компьютерные технологии для реализации своих целей, какие инструменты и методы применяют для осуществления взаимодействия с жертвами и другими субъектами и предметами, вовлеченными в их преступные замыслы, рассмотрим частный случай мошеннических действий, получивший свое собственное, хотя и неформальное название – телефонное мошенничество.

В общих словах телефонное мошенничество заключается в том, что обман потерпевшего осуществляется преступниками дистанционно – с помощью телефонной связи. Однако простое использование стационарных или мобильных телефонов не всегда может обеспечить конспиративность преступной деятельности, а также применение методов социальной инженерии, например когда для обмана потерпевшего требуется сокрытие телефонного номера звонящего либо его подмена при определении входящего звонка. Для реализации таких замыслов преступники используют возможности *IP*-телефонии (технология *VoIP – Voice over Internet Protocol*). Сама по себе *IP*-телефония как технология (сетевые протоколы, ПО) является достаточно простой, однако ее использование совместно с иными интернет-технологиями, например *VPN* (*Virtual Private Network* – виртуальная частная сеть), предоставляет мошенникам широчайшие возможности для сокрытия следов преступной деятельности и применения методов психологического воздействия на потерпевших. Манипулируя различными технологическими инструментами, преступники, как из элементов конструктора *LEGO*, моделируют многообразные схемы телефонной коммуникации.

В основе всех схем находится непосредственно протокол *VoIP*, реализация которого схожа с функционированием электронной почты. Клиенты сервисов IP-телефонии имеют свои адреса, например *12345@voip.ru*. Когда с абонентом пытается связаться клиент другого сервиса, первоначально запрос на голосовой вызов поступает на прокси-сервер, который определяется по имени домена – *voip.ru*. Прокси-сервер проверяет, зарегистрирован ли на сервисе абонент с таким именем, и при положительном результате перенаправляет запрос на свой же *SIP*-сервер, который содержит постоянно обновляющуюся таблицу *IP*-адресов устройств клиента, на которые он ожидает вызова. Первое устройство из списка, которое ответило на вызов, по-

лучив запрос от вызывающего абонента с указанием его *IP*-адреса и иных технических данных, в ответ отправляет свои данные, включая *IP*-адрес. После того, как абоненты договорились о коммуникации, голосовой трафик осуществляется напрямую между оконечными устройствами, минуя серверы провайдеров *IP*-телефонии. В этой достаточно прозрачной схеме источники, содержащие криминалистически значимую информацию, очевидны – это прокси-серверы и *SIP*-серверы провайдеров *IP*-телефонии, а также непосредственно оконечные устройства, в качестве которых могут использоваться смартфоны, *IP*-телефоны, компьютеры пользователей. Соответственно, достаточно истребовать у провайдеров *IP*-телефонии информацию о телефонных запросах на голосовые соединения и ответы на них, а также сведения из таблиц *SIP*-серверов, чтобы установить абонентов. Однако, осознавая, что применение простой схемы приведет к их скорому разоблачению, мошенники обычно дополняют ее следующими элементами (*рис. 3.7–3.8*):

- прокси-серверы и *VPN*-серверы, шифрующие голосовой трафик и скрывающие адреса оконечных устройств;
- пограничное оборудование, позволяющее организовывать телефонные соединения между абонентами общетелефонной сети и *IP*-телефонии;
- виртуальные АТС, разделяющие сегменты многоэлементной сети IP-телефонии.

Если использование в преступных целях прокси-серверов и сетей *VPN* не раз упоминается в настоящем пособии, то на двух других пунктах следует остановиться подробнее.

Рис. 3.7. Схема анонимизации *call*-центра с использованием *VPN*

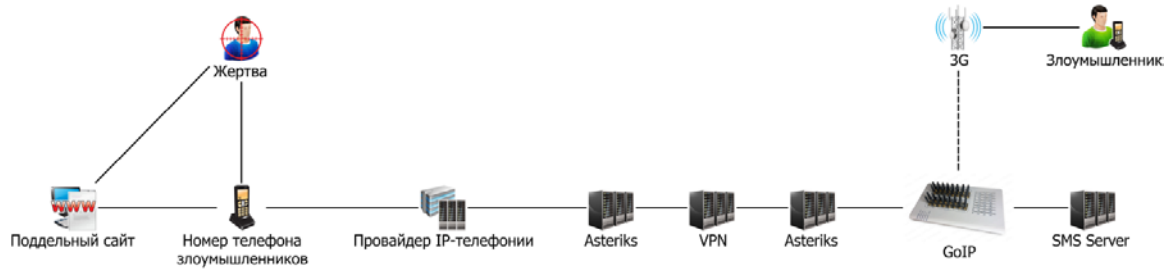


Рис. 3.8. Схема анонимизации с несколькими узлами

Абоненты *IP*-телефонии имеют возможность использовать номера общетелефонной сети либо посредством их аренды у провайдеров услуг телефонии, которые владеют необходимым оборудованием и телефонной номерной емкостью, либо путем самостоятельной настройки *GSM*-шлюзов, снабженных *SIM*-картами операторов сотовой связи, которые транслируют телефонные соединения в компьютерную сеть и обратно (*рис. 3.9)*.

Рис. 3.9. *GSM*-шлюз, поддерживающий 32 *SIM*-карты

Дальнейшая коммутация вызовов, поступающих на *GSM*-шлюзы, настраивается с помощью виртуальных АТС, одна из самых распространенных реализаций – АТС на базе свободно распространяемого ПО *Asteriks*.

Виртуальная АТС позволяет не только скрыть адреса оконечных устройств, но и осуществлять подмену номера при исходящем звонке путем заполнения поля *CallerID*. В этой связи необходимо отметить, что в отличие от российского законодательства, требующего от оператора связи обязательного подтверждения абонентом владения номером, вводимым им в поле *CallerID*, регламенты проверки номеров провайдерами в некоторых иностранных государствах позволяют использовать любые номера без подтверждения. Так, в случае указания в данном поле номера телефона службы поддержки некоего банка, исходящий вызов, транслированный в общетелефонную сеть через пограничное оборудование на территории иностранного государства, поступив на телефон российского пользователя, отобразится в подмененном виде, то есть вызываемый абонент будет уверен, что ему позвонил представитель банка. Вследствие огромного количества телефонных номеров, использующихся учреждениями банковского сектора для связи с клиентами, отслеживать их с целью выявления подмененных не представляется возможным.

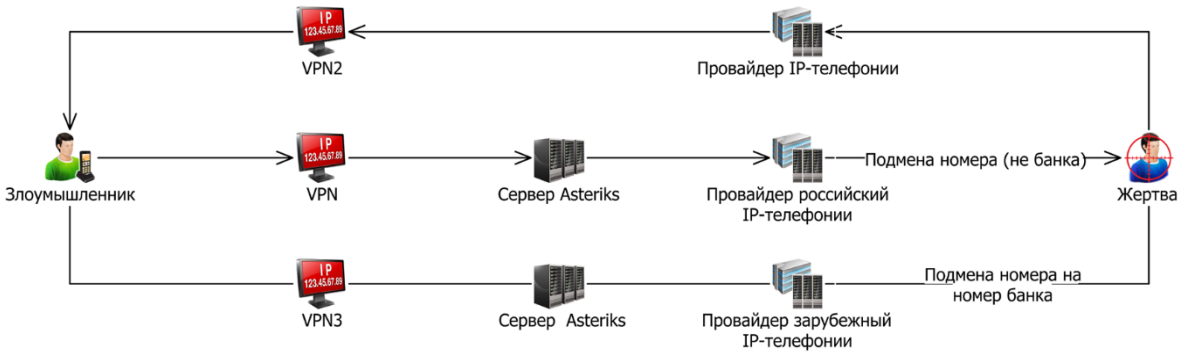


Рис. 3.10. Схема использования *IP*-телефонии с подменой номеров

Приведена мошенническая схема с использованием IP-телефонии, направленная на владельцев банковских карт. Задействованы две нити анонимизации: для входящих и исходящих вызовов с подменой номера исходящего звонка (*рис. 3.10*).

На сегодняшний день операторами связи успешно блокируются только подмены на короткие номера, а также подменные звонки, поступающие с телефонов из номерных емкостей служб поддержки крупнейших банков, которые вкладывают значительные средства в обеспечение безопасности своих клиентов, например «Сбербанка России».

Подводя итог сказанному, необходимо признать, что расследование преступлений, связанных с использованием *IP*-телефонии, несмотря на кажущуюся простоту, – это рутинный и кропотливый труд, эффективность которого можно значительно повысить привлечением к расследованию специалистов в сфере информационной безопасности. Хотя телефонное мошенничество совершается без применения вредоносных программ и не требует несанкционированного доступа к компьютерам потерпевших, методика поиска и сбора цифровых следов преступления идентична применяемым методикам при расследовании преступлений в сфере компьютерной информации, поскольку и в том, и в другом случае в качестве средств совершения преступлений выступают компьютерные системы и их сети.

Тем не менее, невзирая на все возрастающее использование компьютерных технологий при совершении любых преступлений, наиболее массовыми в настоящее время являются преступные посягательства, связанные с хищениями в электронных платежных системах, поэтому рассмотрению способов их совершения, закономерностей развития, методики расследования и тактических особенностей производства отдельных следственных действий по ним необходимо уделить особое внимание. С другой стороны, рассмотрение вопросов

расследования всех возможных видов киберпреступлений представляется нецелесообразным, так как вне зависимости от квалификации таких деяний в процессе доказывания применяются одни и те же приемы и методы. Это обусловлено тем, что преступные действия совершаются не в реальном мире, а в виртуальном – в сфере цифровой информации, хранение, обработка и обращение которой осуществляются посредством вычислительных устройств и их сетей и компьютерных программ.

ГЛАВА 4. ХИЩЕНИЯ В ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ

4.1. Способы совершения преступлений в электронных платежных системах

В предыдущей главе хищения в электронных платежных системах были условно разделены на три группы на основе данных о способах их совершения, методах несанкционированного проникновения в компьютерные системы и их сети и распространения в них, об использовании вредоносного ПО и эксплуатации как программных уязвимостей, так и недостатков организационно-технического характера.

Необходимо отметить, что под угрозой компьютерной атаки находится любая система, которая является заменителем расчетов наличными деньгами при осуществлении внутренних и международных платежей, будь то банковская или иного профильного института. Однако количество преступных посягательств в отношении электронных банковских систем значительно превосходит атаки на иные платежные системы и сервисы. Кроме того, атаки на электронные банковские системы более разнообразны и изощреннее, поскольку преступникам постоянно приходится преодолевать принимаемые банками и производителями банковского ПО меры защиты. Поэтому наиболее полно особенности совершения хищений в электронных платежных системах раскрываются на примере электронных банковских систем, к которым можно отнести и инфраструктурные сетевые ресурсы, обеспечивающие взаимодействие с пользователями, и внутренние сервисы, и клиентов ДБО, и сети банкоматов.

Компьютерным атакам с целью хищения денежных средств подвергаются как внутренние сетевые банковские ресурсы и сервисы, так и компьютерные системы, и сети клиентов ДБО, но источник атаки может быть разным: внешний либо внутренний.

Способы совершения преступлений в платежных системах:

– внешняя атака на сетевую инфраструктуру кредитно-финансовой организации либо на клиентскую часть системы дистанционного банковского обслуживания;

– атака изнутри пострадавшей организации с участием ее работников;

– комбинированная атака, сочетающая в себе элементы обоих указанных выше способов совершения преступления.

Необходимо учитывать, что преступник, действующий внутри организации, может также использовать вредоносные программы, как и преступник внешний. С одной стороны, это усиливает его возможности, с другой – может ввести в заблуждение следствие относительно участия в преступлении инсайдера, если такие программы будут обнаружены в ходе осмотра места происшествия и при проведении судебной экспертизы. Участие инсайдера в преступлении не обязательно должно быть непосредственным. Работник организации может предоставить соучастникам необходимые сведения для осуществления несанкционированного доступа внутрь корпоративной компьютерной сети или сообщить об уязвимостях ПО, установленного на компьютерах организации, либо ошибках в настройках сетевого оборудования.

Современные сетевые технологии позволяют широко использовать в преступных целях удаленный доступ к целевой системе, который с одной стороны предоставляет практически те же возможности, что и непосредственная работа с системой, с другой – дает значительные преимущества преступнику, как то: соблюдение мер конспирации, преодоление физического ограничения доступа к месту планируемого преступления, проведение подготовки к его совершению в течение длительного времени и т. п. Вместе с тем актуальным, хотя и в меньшей степени, остается и способ совершения преступления путем непосредственного доступа к системе (привлечение инсайдеров, незаконное проникновение за охраняемый периметр организации, реализация преступного умысла служащими самой организации).

Данные по способу логического доступа к системе:

– преступления, связанные с удаленным доступом к компьютерному устройству посредством использования компьютерной коммуникационной сети (локальной или глобальной интернет-сети);

– преступления, связанные с непосредственным доступом к компьютерному устройству, в том числе к банкоматам.

Функциональные возможности вредоносных программ и легальных условно опасных программ, предоставляющих удаленный доступ к системе, позволяют проводить атаки на компьютерные системы без какого-либо вовлечения в этот процесс потерпевших. В этом случае реализация преступного умысла осуществляется втайне от них, а зачастую скрыта и от третьих лиц, так как происходит только на уровне машинной обработки и передачи компьютерной информации. В дру-

гих случаях вовлечение потерпевшего в той или иной степени является необходимым условием доведения преступных намерений до конца. При таких обстоятельствах преступники применяют навыки так называемой социальной инженерии, то есть системы психологических приемов и методов, склоняющих потерпевших к совершению определенных действий в их интересах, например к разглашению уникального кода, присланного в *SMS* для подтверждения финансовой операции. Непосредственная эксплуатация уязвимостей человеческого фактора предусматривает прямое общение с потерпевшим с применением навыков социальной инженерии. Однако низкий уровень культуры информационной безопасности позволяет преступникам получать необходимые сведения для проведения атаки и без прямого общения с потерпевшим. Использование ненадежных паролей, заводских настроек и конфигураций ПО и оборудования предоставляет широкий спектр возможностей для получения несанкционированного доступа к конфиденциальной информации. Для доступа к корпоративным компьютерным системам преступники могут воспользоваться и уязвимостями в организации охранных систем и регламентов предприятия, что может выражаться как в физическом проникновении за охраняемый периметр, так и в удаленном доступе с использованием разрешенных в организации к применению протоколов и программных средств.

Способы проникновения в систему:

– эксплуатация уязвимостей аппаратного и программного обеспечения;

– использование недостатков организационного и технического характера корпоративных охранных систем;

– применение методов социальной инженерии.

4.2. Функциональные возможности современных вредоносных программ

К настоящему времени одноповеденческие вредоносные программы, функциональность которых охватывала бы только конкретный вид действия, например поиск платежной информации либо перехват вводимых пользователем паролей, вытеснены с киберкриминального рынка универсальным вредоносным ПО, предоставляющим преступникам практически неограниченные возможности несанкционированного доступа к компьютерной информации и воздействия на нее.

В широком понимании любая троянская программа представляет собой комплекс вредоносного ПО, состоящий из серверной части – управляющей и клиентской части – программы-бота. Но на современном этапе развития понятие – комплекс вредоносного ПО – приобрело новый смысл. В большинстве троянских программ, использующихся при совершении хищений в электронных платежных системах, разработчики реализуют модульную архитектуру. Каждый модуль отвечает за конкретный вид действия, но на зараженном компьютере может работать только во взаимодействии с главным модулем – ядром.

Порядок загрузки и установки на компьютер троянской программы обычно выглядит следующим образом.

На первом этапе в компьютерную систему внедряется программа-загрузчик (*Trojan-Downloader* – по классификации детектируемых объектов «Лаборатории Касперского»). Осуществляется это одним из способов, рассмотренных выше, основные из которых – атака набором эксплойтов либо заражение через вредоносное вложение в электронном письме.

В общем случае программа-загрузчик должна выполнить следующие функции: скрыть свое появление от антивирусного ПО, преодолеть возможные ограничения на исполнение сторонних программ в системе, обратиться на определенный адрес в сети Интернет и загрузить с него основной модуль троянской программы. Иногда разработчики могут предусмотреть дополнительные возможности, например предварительного изучения информации на наличие в системе программ ДБО, по результатам которого программа либо самоуничтожается, либо выполняет свою основную задачу – загружает троянскую программу.

Если для выполнения своей основной задачи программе-загрузчику достаточно отработать исключительно в оперативной памяти без записи в дисковое пространство, то есть один цикл до перезагрузки компьютера, основной модуль программы-бота в большинстве случае сохраняется на жесткий диск, чтобы обеспечить длительный период присутствия в системе пользователя. Одновременно определенным образом модифицируются файлы ОС, чтобы обеспечить запуск вредоносной программы каждый раз при включении компьютера.

Собранную основным модулем информацию о компьютерной системе пользователя троянская программа отправляет на управляю-

щий сервер, информация обрабатывается по заданным правилам автоматически либо в ручном режиме оператором центра управления бот-сетью.

Центр управления бот-сетью – это сайт (веб-панель), являющийся элементом комплекса вредоносного ПО и предназначенный для управления вредоносными программами, которыми заражено большое количество компьютеров, а также для накопления, систематизации и анализа переданной с них информации.

По результатам анализа собранной основным модулем информации о системе центр управления отдает команду: загрузить на компьютер дополнительные модули, необходимые для реализации преступного умысла на хищение денежных средств.

Перечень дополнительных модулей определяется на основе анализа следующей информации:

– версия ОС;
– наличие антивирусного ПО;
– наличие программ-клиентов ДБО либо признаков подключения к онлайн-банкингу;
– наличие программ-клиентов иных платежных систем либо признаков подключения к онлайн-сервисам таких систем;
– использование криптографических аппаратных токенов;
– наличие подключенных криптографических аппаратных токенов;
– наличие программ бухгалтерского учета;
– наличие программ удаленного управления и т. п.

Преступные деяния, связанные с хищениями в электронных платежных системах, характеризуются исключительной нацеленностью лиц, их совершающих, на достижение преступного результата. Широкие функциональные возможности современных троянских программ позволяют преступникам реализовать целый набор способов осуществления несанкционированных финансовых операций, несмотря на постоянно совершенствующиеся меры противодействия этому, принимаемые банками и разработчиками ПО.

Способы осуществления несанкционированных операций:

– формирование несанкционированных платежных поручений на компьютере пользователя с помощью программ удаленного управления и отправка их в банк;

– формирование несанкционированных платежных поручений на компьютере преступника посредством доступа к аккаунту ДБО с использованием похищенных аутентификационных данных пользователя и отправка их в банк;

– несанкционированное изменение в ручном либо автоматическом режиме реквизитов получателя в уже сформированном пользователем шаблоне платежного поручения, ожидающем отправки в банк по расписанию;

– несанкционированная автоматическая замена реквизитов получателей в платежных поручениях, экспортируемых пользователем из программ бухгалтерского учета в программу-клиент ДБО для отправки в банк.

Выбор способа совершения хищения зависит от конкретных обстоятельств, например наличия данных об использовании аппаратного токена для идентификации пользователя в системе ДБО, о подключенной опции подтверждения платежных операций с помощью уникального кода, присылаемого в *SMS* на доверенный номер телефона, об установленных программах бухгалтерского учета и т. д. При этом разработчики вредоносных программ и лица, использующие их при совершении преступлений, находятся в постоянном поиске новых способов хищения и их практической реализации.

Такой подход на определенном этапе развития киберпреступности привел к существенному расширению функциональных возможностей вредоносного ПО, позволяющих эффективно атаковать не только компьютеры физических лиц, но крупные корпоративные сети. Примерно с 2014 г. регулярные хищения, связанные с несанкционированным доступом к компьютерной информации, стали совершаться в кредитно-финансовых учреждениях.

Способы совершения хищений, реализующих несанкционированный доступ к сетевым ресурсам и сервисам банковских компьютерных сетей, представляется необходимым рассмотреть более детально на примере применения комплекса вредоносного ПО Carbanak (*рис. 4.1*).

По результатам исследования , проведенного Лабораторией Касперского, было установлено, что в основе программного кода комплекса заложен код троянской программы-банкера Carberp, используемой многими преступными группами. Однако разработчики нового вредоносного ПО нагрузили основную троянскую программу дополнительными модулями, которые модернизировали родительскую программу до уровня полнофункционального инструмента, предна-

значенного для комплексных целевых атак на хорошо защищенные корпоративные компьютерные сети.

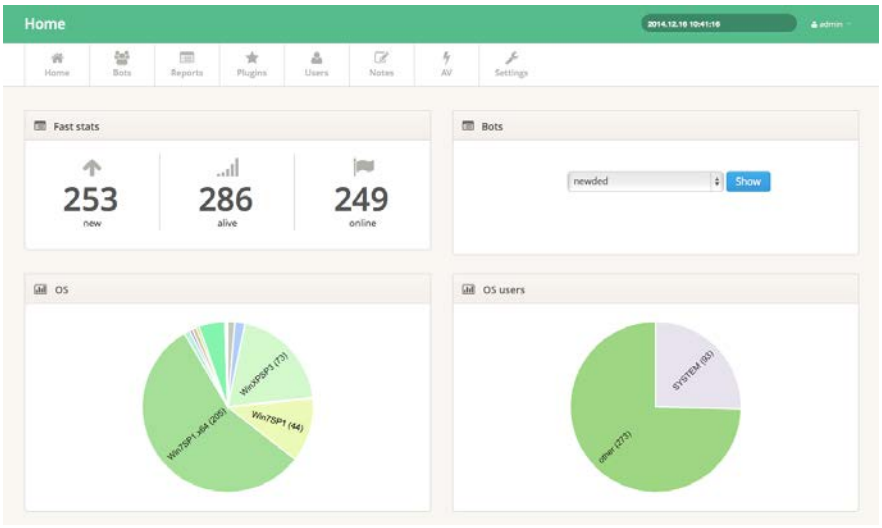


Рис. 4.1. Главная страница панели управления вредоносного ПО *Carbanak*

С начала 2014 г. сетевые ресурсы более 35 российских и европейских банков подверглись заражению этой троянской программой, в результате чего им был причинен ущерб, исчисляемый десятками миллионов долларов.

Расследование обстоятельств хищений позволило детально изучить способ совершения преступлений, в том числе механизмы функционирования вредоносной программы и сценарий действий лиц, ее использующих.

Во всех известных случаях проникновение во внутренние сети осуществлялось с применением методов социальной инженерии посредством рассылки вредоносных писем, вложение к которым содержало документ, преимущественно с расширением *.doc*. Рассылка писем велась как от имени физических лиц – клиентов банка, так и от лица регулирующих органов.

Изученные вредоносные письма содержали соответствующие вложения со следующими именами:

- «Соответствие ФЗ-115 от 24.06.2014г.doc».
- «Соответствие ФЗ-115 от 21.07.2014г.doc».
- «Соответствие ФЗ-115 от 02.07.2014г..doc».
- «Уведомление Центрального Банка РФ от 04.08.2014.scr».
- «Запрос.doc».
- «new.doc».
- «Анкета – Заявление.doc».
- «Приглашение.msg».
- «Приглашение.doc».

При попытке открытия файла пользовательский компьютер подвергался атаке набором эксплойтов, эксплуатирующих уязвимости приложения *Microsoft Word*. В случае срабатывания хотя бы одного из них из файла извлекался скрытый в нем в зашифрованном виде вредоносный код и в скомпрометированную систему устанавливалась вредоносная программа *Carbanak*. Для сокрытия нахождения в системе программа маскировала свой исполняемый файл под системный и внедряла вредоносный код в системные процессы *Windows*.

После успешной установки программа отправляла зашифрованное уведомление серверу управления, содержащее информацию о зараженном компьютере и зарегистрированных на нем пользователях, по протоколу *HTTP*, который используется веб-браузерами для работы в сети Интернет и, как правило, разрешен на пользовательских машинах.

Проникнув во внутреннюю сеть и закрепившись хотя бы на одной машине, атакующие приступали к изучению структуры сети. Как правило, для успешной реализации этого этапа атаки преступникам требовалось перехватить аутентификационные данные учетной записи администратора домена, что позволило бы осуществлять доступ ко всем элементам сетевой инфраструктуры с наивысшими привилегиями, в том числе к компьютерам любых пользователей сети, почтовым серверам, серверам баз данных и автоматизированных банковских систем.

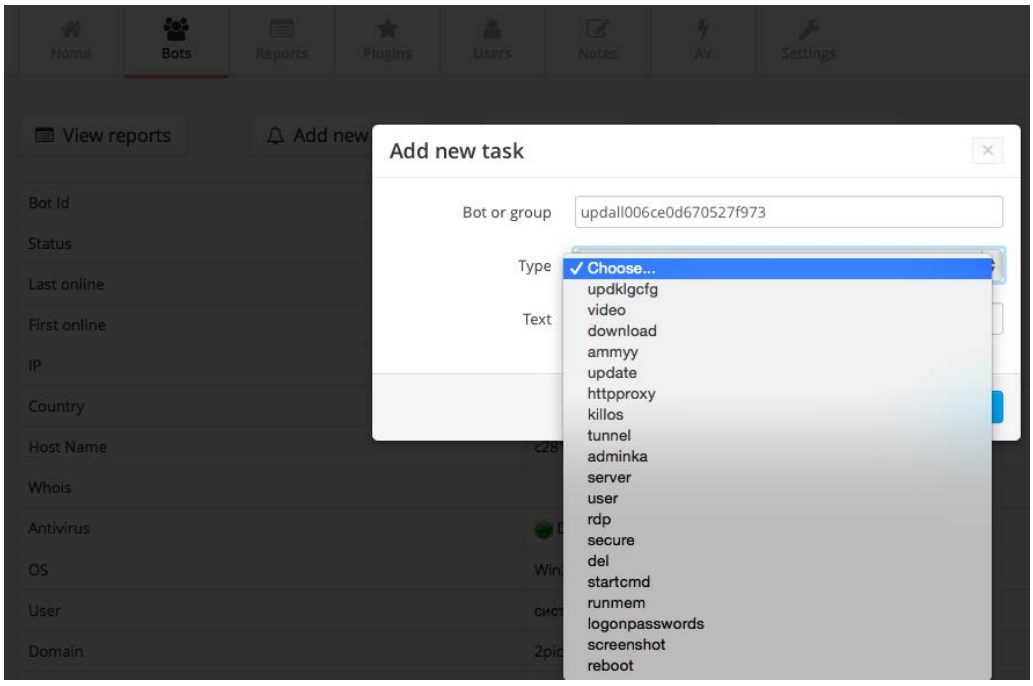


Рис. 4.2. Добавление задачи программе-боту в панели управления вредоносного ПО *Carbanak*

Решение этой задачи (*рис. 4.2*) осуществлялось с помощью специализированных модулей, входящих в состав комплекса ПО *Carbanak* (*рис. 4.3*):

– *Mimikatz* – утилиты, предназначенной для получения паролей пользователей ОС *Windows*, вошедших в систему;

– *Meterpreter* – программы для скрытого удаленного управления компьютером, содержащей обширный набор инструментов для исследования сети, записи сетевого трафика и экрана, повышения привилегий пользователя, удаленной загрузки исполняемых файлов и их запуска;

– *Ammyy Admin* – системы удаленного администрирования, позволяющей получить доступ к компьютеру или серверу, подключения к которым из внешней сети запрещены политиками безопасности;

– *HVNC Server* – программы, обеспечивающей скрытое подключение к компьютеру. В случае если политиками безопасности подключение из внешней сети запрещено, программа обладает функциональностью обходить эти ограничения;

– *Keylogger* – модуля, регистрирующего нажатия на клавиатуре, что позволяет перехватывать вводимую пользователем информацию, в том числе пароли.

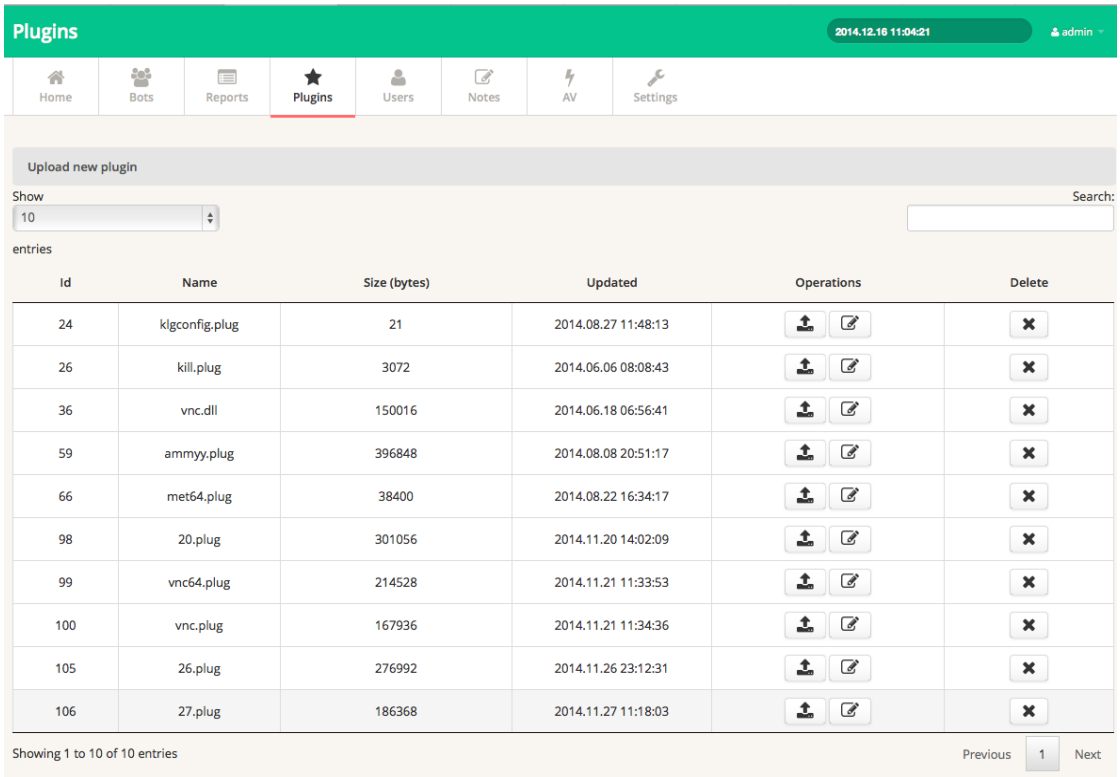


Рис. 4.3. Список установленных модулей вредоносного ПО *Carbanak*

Закрепившись в системе, преступники запускали модуль *Ammyy Admin*. В случае успешной инсталляции программа сообщала серверу управления идентификатор (*AmmyyID*), использование которого позволяло осуществить подключение в обход ограничений, предусмотренных политиками безопасности. В результате атакующие получали инструмент для детального исследования удаленной системы.

Кроме того комплекс *Carbanak* обладал возможностью производить запись экрана, что позволяло преступникам наблюдать за экраном глазами пользователя, оценивая круг его задач, контактов, используемые им банковские приложения, последовательность действий.

Для выявления пользователей, имеющих административные права и доступ к интересующим их ресурсам, преступники использовали в настройках модуля *Keylogger* фильтр «по ключевым словам» (*рис. 4.4*). При обнаружении процессов, соответствующих фильтру, автоматически включалась регистрация нажатий клавиш клавиатуры и начинали производиться снимки экрана.

Таким образом, преступники собирали информацию о пользователях, уровне их доступа, именах учетных записей и паролях, а также изучали алгоритмы работы в банковских приложениях.

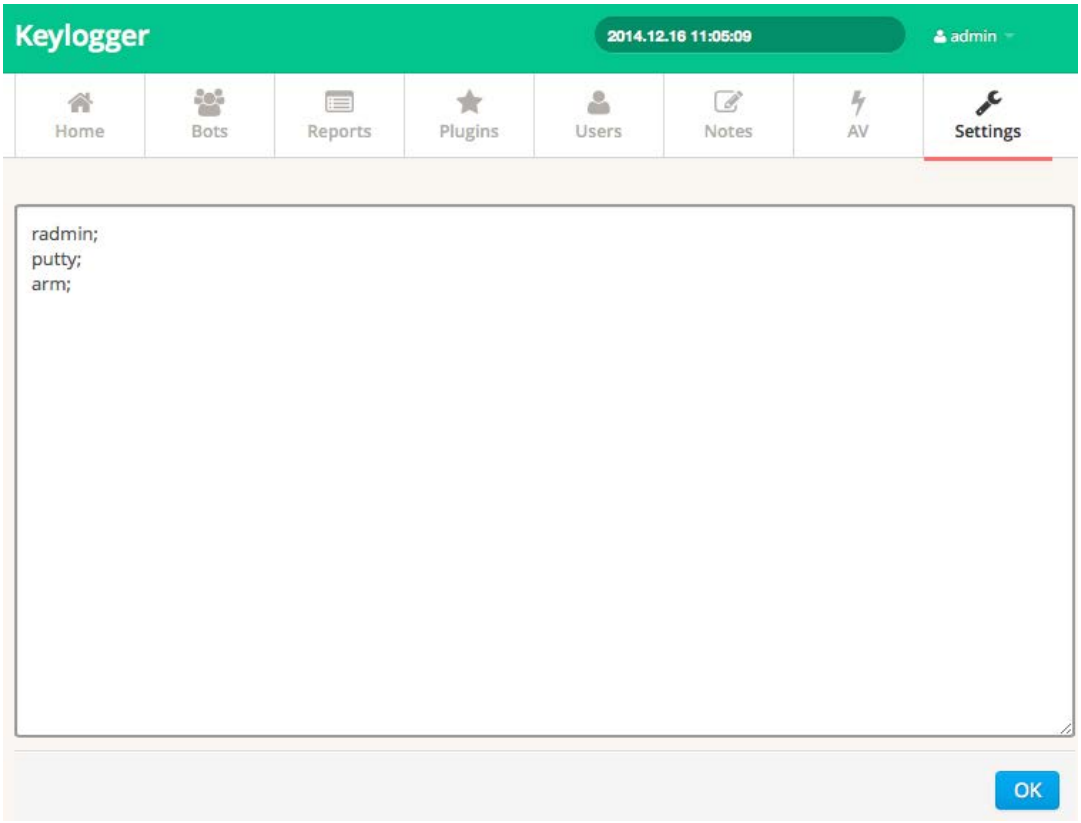


Рис. 4.4. Пример использования фильтра «по ключевым словам» в настройках модуля *Keylogger*

Процесс исследования сети и сбора информации продолжался длительный период времени – около полугода и более с момента проникновения в сеть и до несанкционированного списания денежных средств.

В случаях доступа к сетевым ресурсам организаций, не являющихся учреждениями кредитно-финансового сектора, несанкционированные платежи осуществлялись способами, рассмотренными выше. Похищенные денежные средства направлялись на счета подставных юридических и физических лиц.

Способы хищения при несанкционированном доступе к сетевым ресурсам и сервисам банковских компьютерных сетей реализуются иным образом.

Способы осуществления несанкционированных операций:

– выдача денежных средств из банкоматов с помощью несанкционированного удаленного управления ими из сети банка;

– выдача денежных средств из банкоматов при обслуживании банковских карт с отмененными либо максимально повышенными в результате несанкционированного воздействия на банковский процессинг лимитами снятия наличных денежных средств;

– замена реквизитов получателей в платежных документах, обрабатываемых компьютерными терминалами – АРМ КБР (автоматизированное рабочее место клиента Банка России) либо *SWIFT* (*Society for Worldwide Interbank Financial Communications* – международная межбанковская система передачи информации и совершения платежей).

Другими актуальными угрозами для учреждений банковской сферы являются хищения денежных средств из банкоматов. В этом случае реализуется иной способ совершения преступления – киберпреступники используют физический доступ к компьютерной системе.

Современные методики и способы, применяемые преступниками при совершении хищений, предусматривают комплексную эксплуатацию уязвимостей как механической, аппаратно-технической частей банкомата, так и ее программной составляющей. Это обусловлено распространенным в настоящее время подходом к обеспечению сохранности денежных средств, помещенных в банкомат: высокая степень защиты сейфового отделения (непосредственно сейф, кодовые замки, сигнализация, датчики различных типов и т. п.) и низкий уровень защищенности инженерного (верхнего) отсека – сервисной зо-

ны; из-за этого преступники могут получить несанкционированный доступ к встроенному в аппарат компьютеру с установленными на нем ОС и прикладными программами, которые управляют работой банкомата.

На первом этапе киберпреступники, используя низкий уровень защищенности сервисной зоны банкомата, получают доступ к компьютеру с установленными на нем ОС *Windows* и прикладным ПО, обеспечивающим функционирование банкомата.

Как показывают результаты расследования хищений денежных средств из банкоматов, защита верхнего отсека ограничивается запиранием дверцы с помощью механического замка; как правило, для всех банкоматов сети используется один унифицированный ключ; нередко сигнализация и датчики, предупреждающие о несанкционированном доступе, не применяются.

Рис. 4.5. Стенд банкомата

Затем, используя уязвимости в базовой системе ввода-вывода (англ. *basic input/output system – BIOS*), в которой по умолчанию заданы параметры приоритета загрузки компьютера с внешних дисков, преступники устанавливают на компьютер под управлением ОС *Windows* вредоносное ПО, например троянскую программу, определяемую антивирусным ПО «Лаборатории Касперского» с именем *Backdoor.MSIL.Tyupkin.a,* путем подключения внешнего носителя с помощью *USB*-интерфейса и перезагрузки компьютера с помощью выведенной на переднюю панель клавиши *Reboot*. После загрузки на компьютер вредоносного ПО необходимость в доступе к сервисной зоне банкомата отпадает, управление компьютером осуществляется путем введения специальных кодов с использованием штатной функциональной клавиатуры (ПИН-пада).

Изображен тестовый стенд банкомата, использовавшийся при проведении исследования (*рис. 4.5*).

Программа *Backdoor.MSIL.Tyupkin.a* обладает функциональностью, позволяющей инициировать процесс выдачи денежных средств банкоматом, отдавая соответствующую команду устройству выдачи денежных купюр банкомата в определенное время и в определенный день недели: в воскресенье или понедельник с 01:00 до 05:00.

Программа способна выполнять следующие команды:

– отобразить окно программы на экране и инициировать процесс выдачи денежных средств банкоматом (для этого на клавиатуре необходимо набрать код «111111»);

– завершить свою работу, удалить свой исполняемый файл и ключ системного реестра для автоматического запуска при загрузке ОС (для этого на клавиатуре необходимо набрать код «333333»);

– установить увеличенный интервал времени, в течение которого программа способна принимать команды с клавиатуры: с 01:00 до 10:00 (для этого на клавиатуре необходимо набрать код «5555555»);

– скрыть окно программы и восстановить сетевое соединение *Local Area Connection* (для этого на клавиатуре необходимо набрать код «000000»).

Ввод кодов команд с клавиатуры должен завершаться нажатием функциональной клавиши с кодом 0x400 (*Enter*).

При наборе на клавиатуре кода «111111» (выдача денежных средств) программа отображает на экране окно, в котором для каждой кассеты выводится следующая информация: номер кассеты, код валюты банкнот, находящихся в кассете, количество банкнот в кассете, сумма денежных средств, находящихся в кассете.

Помимо этого программа выводит на экран код, сгенерированный случайным образом, и строку с предложением ввести сессионный ключ: «*ENTER SESSION KEY TO PROCEED!*». Сессионный ключ генерируется на основе отображенного на экране кода по определенному алгоритму, в котором данный код используется в качестве инициализирующего значения.

Приведен снимок экрана банкомата, зараженного программой *Backdoor.MSIL.Tyupkin.a* (*рис. 4.6*). Устройство находится в ожидании ввода сессионного ключа или кода команды. Если введен правильный сессионный ключ, программа выводит на экран сообщения:

DISABLING LOCAL AREA NETWORK...
PLEASE WAIT...

Рис. 4.6–4.7. Заражение программного обеспечения банкомата

Деактивирует сетевое соединение *Local Area Connection* и предлагает ввести номер кассеты, отображая на экране сообщение:

CASH OPERATION PERMITTED.
TO START DISPENSE OPERATION –
ENTER CASSETTE NUMBER AND PRESS ENTER.

Приведен снимок экрана банкомата с интерфейсом вредоносной программы *Backdoor.MSIL.Tyupkin.a*, ожидающей выбор кассеты для выдачи денег (*рис. 4.7*).

Далее может быть введен номер кассеты либо другие команды. Если введенный код не является командой и не является правильным номером кассеты, программа снова предлагает ввести номер кассеты, отображая на экране сообщение:

CASH OPERATION PERMITTED.
INVALID CASSETTE NUMBER. TRY AGAIN.
TO START DISPENSE OPERATION -
ENTER CASSETTE NUMBER AND PRESS ENTER.

Если был введен правильный номер кассеты, программа выводит на экран сообщение:

CASH OPERATION IN PROGRESS...PLEASE WAIT...

Отдает команду устройству выдачи банкнот выдать 40 купюр или, если в кассете находится меньше 40 банкнот, выдать все оставшиеся.

Затем на экране снова отображается информация о номерах кассет, кодах валют банкнот, находящихся в кассетах, количестве банкнот в кассетах, суммах денежных средств, находящихся в кассетах, а также сообщения:

CASH OPERATION FINISHED.
TAKE THE MONEY NOW!
CASH OPERATION PERMITTED.
TO START DISPENSE OPERATION –
ENTER CASSETTE NUMBER AND PRESS ENTER.

После этого программа ожидает ввода с клавиатуры номера кассеты или кода команды.

Таким образом, хищение денежных средств, хранящихся в банкомате, осуществляется путем ввода соответствующих команд с помощью штатной функциональной клавиатуры. При этом преступные действия и лицо, их производящее, посредством видеозаписи не фиксируются, так как в отсутствие банковской карты в кардридере (устройстве для чтения банковских карт) камера наблюдения банкомата отключена. На заключительном этапе предпринимаются меры к сокрытию следов преступления. Используя функциональность вредоносной программы, киберпреступник производит ее удаление путем ввода с помощью ПИН-пада определенного кода, после чего, осуществив доступ к инженерному отсеку вследствие невысокого уровня его защищенности, производит перезапуск компьютера с помощью клавиши *Reboot*.

На настоящий момент инструментарий троянских программ предоставляет преступникам полный доступ к компьютерным системам и сетям пользователей и контроль над ними, если они не будут обнаружены антивирусным и другим защитным ПО. Поэтому одной из основных задач разработчиков современных вредоносных программ является изыскание новых способов обеспечения скрытого характера их работы.

4.3. Методы сокрытия следов преступления

Меры, принимаемые к сокрытию следов преступлений в сфере компьютерной информации, условно можно разделить на несколько видов. К первому относятся действия по сокрытию киберпреступни-

ками своих данных при использовании сети Интернет с целью предотвращения идентификации их личности. Ко второму виду – меры по сокрытию адресов сетевой инфраструктуры, используемой для осуществления несанкционированного доступа к компьютерам пользователей, управления троянскими программами, распространения вредоносного ПО и др. К третьему виду – сокрытие следов несанкционированного доступа к компьютерам пользователей.

Для сокрытия своего адреса киберпреступники используют различные анонимные компьютерные сети и сервисы, специально созданные для этих целей.

VPN-сервисы – услуга, обеспечивающая шифрование сетевого трафика пользователя между его компьютером и *VPN*-прокси-сервером, который является шлюзом выхода в сеть Интернет и, соответственно, скрывает реальный *IP*-адрес пользователя. Преступники предпочитают сервисы, находящиеся в юрисдикции других государств и не требующие подтверждения персональных данных при регистрации, а также предоставляющие большой выбор стран, где расположены серверы-шлюзы (прокси). Если им требуется более высокий уровень конспирации, киберпреступники могут арендовать у провайдеров хостинговых услуг вычислительные мощности практически в любой точке мира, на которых настриваются собственные *VPN*-серверы либо виртуальные машины, с которых, используя сторонние *VPN*-сервисы, производится выход в сеть Интернет.

Tor (*the onion routing* – луковая маршрутизация второго поколения) – технология и ПО для реализации обмена данными с многослойным шифрованием с помощью системы прокси-серверов, обеспечивающих анонимное сетевое подключение.

Троянская программа, обладающая функциональными возможностями *VPN*-прокси-сервера, позволяет преступникам создать бот-сеть из компьютеров, зараженных такой программой, и использовать их для анонимизации своих сетевых подключений.

Обратной стороной использования анонимных сетей является снижение скорости обмена данными и нестабильность соединения, однако для большинства киберпреступников конспирация их деятельности имеет приоритетное значение.

Помимо использования сетевых технологий для анонимизации подключения к сети Интернет киберпреступники применяют и просто криминальные либо полукриминальные схемы: через несанкционированное подключение к сторонним беспроводным точкам доступа – *Wi-Fi*-

роутерам либо с помощью беспроводных модемов мобильной связи с *SIM*-картами, оформленными на подставных лиц.

Выбор безопасных способов оплаты сервисов и вычислительных мощностей для осуществления преступной деятельности также является мерой конспирации преступной деятельности. Для этих целей широко используется так называемая криптовалюта, например биткоины. В настоящее время активно идет процесс легализации криптовалюты. Однако большинство государств, включая Российскую Федерацию, не признает ее в качестве платежного средства. Фактически криптовалюта рассматривается как средство инвестирования или товар.

Для разработки планов преступной деятельности, координации мероприятий на стадии подготовки к совершению преступления, согласования совместных действий соучастники широко применяют сетевые протоколы обмена сообщениями, обеспечивающими безопасность передачи данных, и, напротив, исключают использование средств коммуникации, позволяющих идентифицировать абонента. Одной из наиболее востребованных реализаций коммуникации в киберкриминальной среде является *XMPP*-протокол обмена мгновенными сообщениями, известный еще как *Jabber*-протокол, который предоставляет возможность настроить свой собственный *Jabber*-сервер, обеспечивающий шифрование канала.

Меры по сокрытию сетевой инфраструктуры, используемой при совершении преступлений в сфере компьютерной информации, сводятся, в основном, к использованию анонимных сетей для организации взаимодействия между ее элементами. Например, взаимодействие серверов управления, которые являются ключевым звеном сетевой инфраструктуры, с компьютерами-ботами настраивают через прокси-серверы провайдеров, находящихся в юрисдикциях разных государств.

К мерам по сокрытию следов преступления можно отнести также способы и средства, с помощью которых киберпреступники оказывают противодействие осмотру и изъятию с их устройств компьютерной информации, имеющей значение для расследования уголовного дела. Эти цели достигаются шифрованием компьютерных данных с помощью специализированного ПО для того, чтобы они не были доступны третьим лицам, либо возможностью быстрого уничтожения таких данных с использованием специальных программ или физических устройств.

Для сокрытия вредоносной активности на компьютере пользователя применяются различные меры технического характера: как прошедшие проверку временем технологии шифрования и обфускации, так и новые приемы и методы.

Способы сокрытия вредоносной активности в системе:

– технологии *Bootkit*;
– технологии *Rootkit*;
– «бестелесная» технология;
– технологии криптования, обфускации и т. п.

В процессе криптования исполняемый код вредоносной программы шифруется, а при обфускации приводится к виду, затрудняющему анализ и понимание алгоритмов его работы. Это осложняет выявление таких программ антивирусным ПО и их исследование специалистами информационной безопасности.

Вредоносные программы, функционирующие только в оперативной памяти компьютера и не сохраняющиеся на энергонезависимые запоминающие устройства, именуют «бестелесными». При отключении питания компьютера, например при его перезагрузке, программа стирается. Такие программы используются преступниками для сокрытия своей активности от антивирусного ПО. Однако при этом у преступников отсутствует возможность длительной подготовки к совершению преступления, так как при каждой перезагрузке компьютера необходимо заново осуществлять проникновение в целевую систему.

Технология *Bootkit* применяется для сокрытия вредоносного кода от антивирусного ПО и получения максимальных привилегий в системе. Для реализации этого способа вредоносной программой модифицируется загрузочная запись *MBR*, которая считывается процессором еще до начала загрузки ОС, а вредоносный код в зашифрованном виде записывается в неиспользуемую ОС область дискового пространства. При включении компьютера загрузчик еще до старта ОС расшифровывает и загружает в оперативную память вредоносный код.

Максимальные права пользователя позволяют применить набор программ *Rootkit*, которые скрывают вредоносную активность в системе: сетевые подключения, процессы, файлы и т. д.

4.4. Следственные версии по делам о хищениях в платежных системах

Один из наиболее важных вопросов, стоящих перед следователем при расследовании преступлений, совершенных посредством неправомерного доступа в корпоративную сеть, – установление возможной причастности работников потерпевшей организации либо иных лиц, которые в силу своих служебных обязанностей имеют доступ к ее конфиденциальной информации и возможность подключения к корпоративной сети. Сложность разрешения этого вопроса усугубляется тем, что современные комплексы вредоносного ПО обладают настолько мощным инструментарием, обеспечивающим проникновение даже в хорошо защищенные локальные сети, что создается ложное впечатление о невозможности проведения такой атаки без привлечения инсайдера.

Вместе с тем выявление вредоносных программ и следов их работы на компьютерах и серверах корпоративной сети не может являться безусловным аргументом, чтобы не рассматривать версию совершения преступления работником пострадавшей организации, тем более при планировании и производстве первоначальных следственных действий. Результаты проведенных впоследствии судебных компьютерных экспертиз могут установить отсутствие причинно-следственной связи между выявленным вредоносным ПО и несанкционированным списанием финансовых средств, но к этому времени возможность отыскания новых доказательств на месте происшествия, например следов рук на клавиатуре терминала банковского процессинга, с которого была отдана команда на выдачу денег банкоматами, будет безвозвратно утрачена.

При таких обстоятельствах, приступая к расследованию преступлений, связанных с доступом в корпоративную компьютерную сеть, внутренним сетевым ресурсам и сервисам организаций необходимо рассматривать обе версии:

– преступление связано с несанкционированным проникновением в корпоративную компьютерную сеть в результате эксплуатации уязвимостей ПО, ошибок сетевых настроек и (или) с применением вредоносных программ;

– преступление совершено работником организации, воспользовавшимся физическим доступом к компьютерам и серверам корпоративной сети.

4.5. Лица, совершающие преступления в сфере компьютерной информации

Преступления в сфере компьютерной информации носят в большинстве случаев групповой характер, что обусловлено совокупностью многих факторов: необходимостью разноплановых специальных познаний в криптографии, сетевых взаимодействиях, программировании, администрировании, технической поддержке и т. п. Кроме того, например, для реализации преступного умысла на хищение с использованием систем ДБО недостаточно знаний только в компьютерной сфере. Необходимо привлечение специалистов в банковской области и иных лиц, обналичивающих похищенные денежные средства. Сотрудничество различных групп, обладающих той или иной преступной специализацией, на протяжении длительного времени приводит к фактическому созданию преступных сообществ. Специфичной формой групповой деятельности в сфере компьютерной информации является партнерство, когда определенный вид преступной деятельности предлагается неопределенному кругу потенциальных соучастников в виде сервиса. Партнерство – одна из форм реализации бизнеса, удачно адаптированная для осуществления преступной деятельности. Варианты партнерских отношений могут быть самыми разнообразными, но в любом случае они направлены на достижение общей преступной цели.

В связи с тем, что преступления в сфере компьютерной информации носят преимущественно групповой характер, соучастие объективно характеризуется таким признаком, как преступная специализация. Помимо специалистов в области компьютерной информации в деятельность преступных групп вовлекаются «смежники», то есть лица, обладающие специальными познаниями в других областях, например в банковской сфере, без участия которых достижение преступного результата становится проблематичным. Для обеспечения высокотехнологичной преступной деятельности привлекается «обслуживающий персонал», обязанностями которого является техническая поддержка сетевой инфраструктуры, компьютерных устройств, а также решение иных рабочих вопросов. В качестве «эксплуататоров» выступают лица, не обладающие специальными знаниями в области компьютерной информации, но в силу своих преступных наклонностей и при наличии денежных средств приобретающие киберкриминальный сервис, предлагаемый в форме партнерства (*табл. 1*).

Таблица 1

Разделение участников преступной деятельности в области компьютерной информации

По форме соучастия	По преступным ролям
одиночки	«спецы»
группы	«обслуживающий персонал»
сообщества	«смежники»
партнерства	«эксплуататоры»

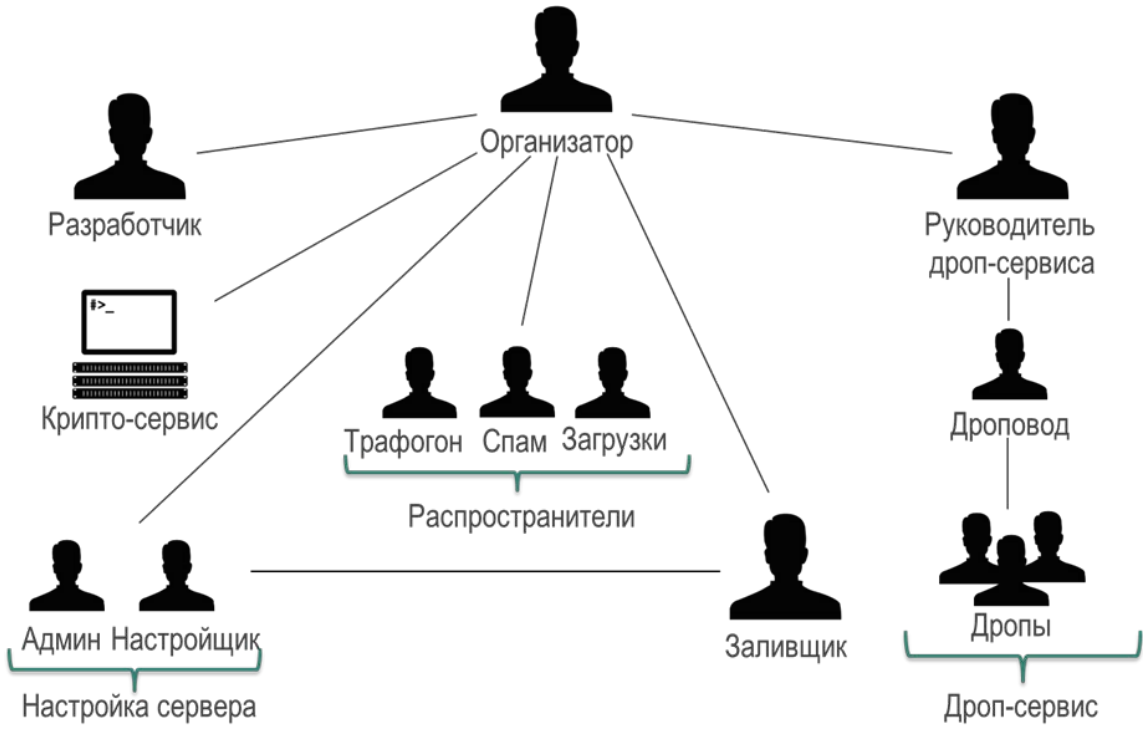


Рис. 4.8. Структура преступной группы, специализирующейся на хищениях

Распределение ролей в преступной группе, как правило, соответствует специализации ее участников (*рис. 4.8*):

– организатор (руководитель группы, координатор различных направлений деятельности ее соучастников);

– разработчик (создатель вредоносного ПО);

– заливщик (оператор центра управления зараженными компьютерами);

– администратор сети (поддержка штатного функционирования сетевой инфраструктуры);

– настройщик веб-интерфейса (поддержка штатного функционирования центра управления);

– криптор (шифрование вредоносного кода с целью противодействия защитному ПО);

– распространитель вредоносного ПО (поддержка функционирования связок эксплойтов, спам-сервиса);

– дроп-сервис (обналичивание похищенных денежных средств).

4.6. Причины и условия совершения преступлений

Как известно, первопричиной преступности являются свойства личности и ее состояние в конкретных жизненных условиях. Формирование личности на современном этапе происходит на фоне развития компьютерной техники и цифровых технологий, доступности компьютерных устройств и сервисов сети Интернет практически любому жителю большинства стран мира. Реализация планов цифровизации экономик ведущих государств, в том числе России, приводит к перемещению всех видов финансово-хозяйственной деятельности и социального взаимодействия в виртуальное пространство. Соответственно, происходит цифровизация общественных отношений. Следуя этим тенденциям, преступная деятельность также перемещается в информационно-коммуникационную сферу. Все чаще при совершении преступлений общеуголовной направленности используются компьютерные устройства и сервисы сети Интернет, преступники осваивают новые сетевые технологии и компьютерные программы и применяют их в качестве средств и орудий преступлений. Отсутствие личного контакта с потерпевшим, а также относительная легкость совершения преступного посягательства являются дополнительными катализаторами киберпреступности.

Для оптимизации извлечения преступных доходов криминалом востребованы новые бизнес-технологии, ставшие доступными благодаря свободе обращения информации в сети Интернет. Например, форма совместной деятельности в виде партнерства активно используется при подготовке и совершении киберпреступлений.

На таком фоне имеющиеся возможности противодействия противоправным проявлениям в виртуальном пространстве, в том числе киберпреступной деятельности, не соответствуют уровню современных угроз. Как видится, основная причина этого в том, что законодателем неправильно оценены риски. Так, при осуществлении финансовых операций непосредственно в отделении банка личность

клиента подтверждается предъявлением соответствующих документов, позволяющих его идентифицировать, то есть, по существу, проводится биометрическое распознавание клиента. Вместе с тем Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» при осуществлении платежей с использованием платежных банковских карт и посредством ДБО предусмотрена упрощенная идентификация клиента (введение ПИН-кода, пароля, электронной цифровой подписи), которая фактически является процедурой аутентификации. Таким образом, подмена понятий, когда вместо биометрической идентификации, ответственность за соблюдение которой возложена на кредитную организацию, предусмотрена процедура простой аутентификации, приводит к неправильному распределению рисков, поскольку после ее прохождения ответственность за последствия, в том числе за несанкционированные финансовые операции в системе ДБО, перекладывается на пользователя.

Возложение основных рисков в сфере использования высоких технологий на конечных потребителей информационных продуктов и услуг, не имеющих возможностей оказывать какое-либо существенное влияние на повышение их безопасности и разработку средств защиты, препятствует принятию реально действенных мер.

Значительное влияние на создание условий преступности оказывает виктимологический аспект. Недостаточная информированность пользователей об угрожающих возможностях, которыми сейчас обладает киберпреступность, и пренебрежительное, легкомысленное отношение к необходимости соблюдения правил информационной безопасности служат дополнительной мотивацией к развитию преступных проявлений.

Приведены статистические данные[1], позволяющие представить степень латентности преступности в сфере компьютерной информации (*табл. 2*). Таблица содержит сведения о количестве осужденных лиц по преступлениям в сфере компьютерной информации и хищениям, совершаемым с использованием информационно-коммуникационных технологий по данным официального сайта Судебного департамента при Верховном Суде Российской Федерации (форма № 10-а).

---

[1] Данные судебной статистики [Электронный ресурс] // Судебный департамент при Верховном Суде Российской Федерации // URL: http://www.cdep.ru/index.php?id=79.

Таблица 2

Количество осужденных лиц по ст.ст. 159.3, 159.6, 272–273 УК РФ, 2015–2018 гг.

Статья УК РФ	2015	2016	2017	2018
159.3	154	84	79	239
159.6	88	124	144	54
272	71	62	75	50
273	164	123	128	79

Приведены данные о количестве уведомлений об обнаружении антивирусным ПО «Лаборатории Касперского» троянских программ-банкеров, троянских программ-шифровальщиков, троянских программ, предназначенных для DDoS-атак, троянских программ под ОС *Android* за период с 2012 по 2018 гг. (*рис. 4.9–4.12*).

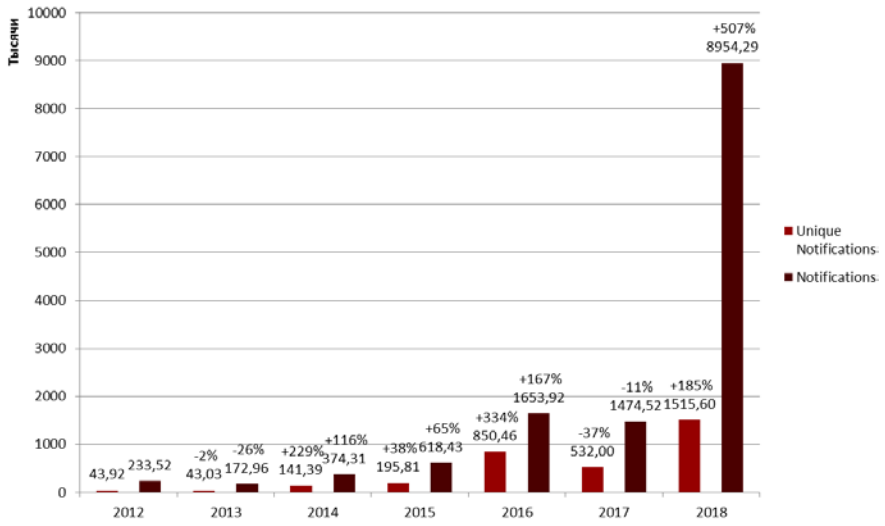


Рис. 4.9. Обнаружение троянских программ-банкеров

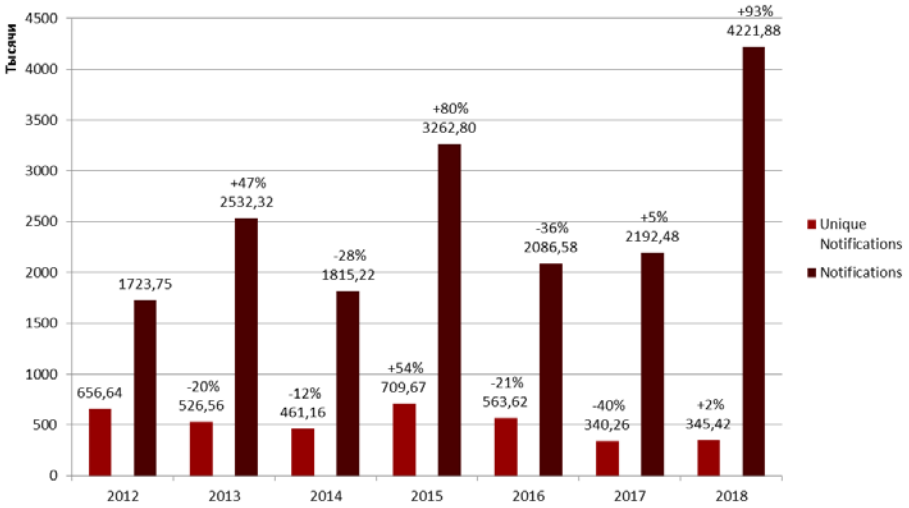


Рис. 4.10. Обнаружение троянских программ-шифровальщиков

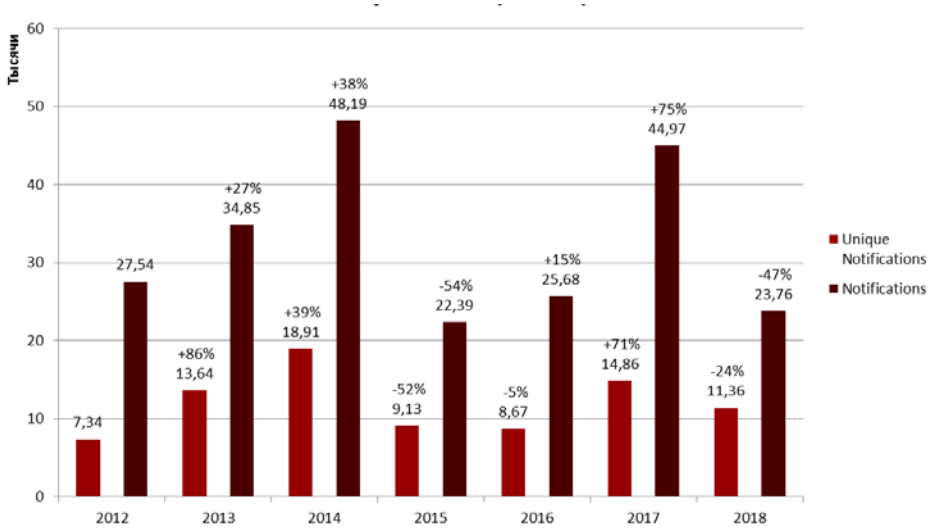


Рис. 4.11. Обнаружение троянских программ, предназначенных для *DDoS*-атак

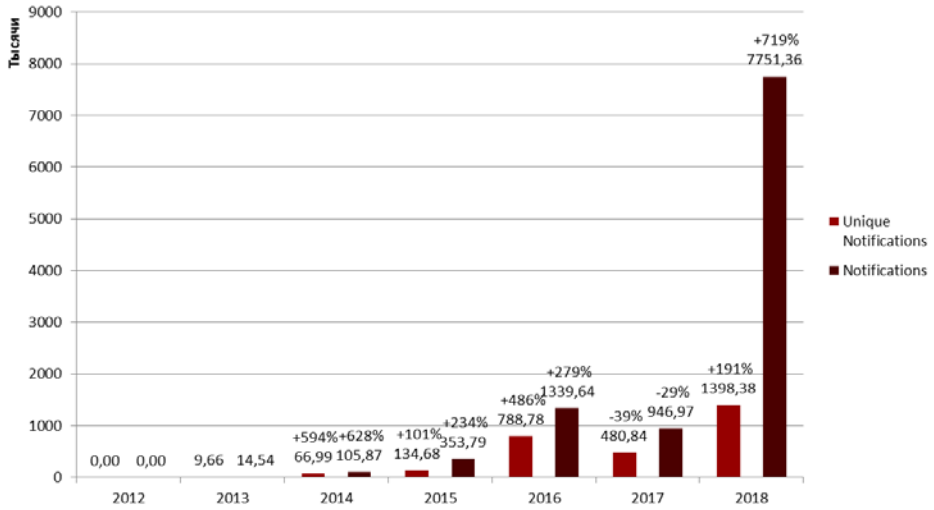


Рис. 4.12. Обнаружение троянских программ под ОС *Android*

Можно сделать вывод, что бурному развитию киберпреступности способствует неготовность современного общества к оказанию эффективного предупредительного противодействия. Криминологическая наука до сих пор не располагает достоверными сведениями о состоянии, уровне и структуре рассматриваемой преступности, а в теории уголовного права и в правоприменительной практике нет единства взглядов по поводу уголовно-правовой оценки преступлений, включенных в орбиту киберпреступности. В связи с этим значительная часть общественно опасных проявлений киберпреступности остается за пределами мер уголовно-правового реагирования, что является благодатной почвой для ее самодетерминации.

ГЛАВА 5. КИБЕРТЕРРОРИЗМ

И мировое сообщество в целом, и национальные правоохранительные органы большинства развитых стран в частности изначально осознавали, насколько серьезную угрозу представляет использование террористическими организациями глобальной сети Интернет, ее ресурсов и сервисов. Новые возможности распространения и сбора информации по всему миру, широчайший доступ к аудитории, различные способы коммуникации, в том числе с применением шифрования, пропаганда своих идей и вербовка новых членов, оказание массового психологического воздействия и широкий спектр иных возможностей, предоставляемых современными высокими технологиями в информационно-телекоммуникационной сфере, обусловили появление в современном обществе такого негативного и чрезвычайно опасного явления, как кибертерроризм. Вместе с тем, несмотря на осознание исходящей от него угрозы, вследствие продолжающегося бурного развития информационных технологий и быстро меняющейся обстановки мировому сообществу не всегда удается своевременно выработать и реализовать адекватные и эффективные меры противодействия его проявлениям.

Способы использования сети Интернет террористическими организациями:

– пропаганда и распространение радикальных идеологических концепций и экстремистских идей по всему миру;

– психологическое воздействие на общество и власти;

– привлечение новых членов в террористические организации;

– сбор информации в террористических целях;

– сбор денежных средств и финансирование террористической деятельности;

– коммуникация между структурами и членами террористических организаций, управление и координация действий;

– приобретение технических средств, материалов и веществ в террористических целях.

Очевидно, что террористы в своей деятельности используют те же возможности глобальной сети и современных компьютерных технологий, что и обычные киберпреступники, за исключением того, что ими не скрываются результаты совершенных ими преступлений, а напротив, последствия проведенного террористического акта предаются максимальной огласке. Целью террористической деятельно-

сти, как следует из диспозиции ст. 205 УК РФ, является дестабилизация деятельности органов власти и международных организаций либо воздействие на принятие ими решений. Для достижения преступного результата террористы с целью устрашения населения совершают деяния, представляющие особую общественную опасность, и тем самым вызывают широкий резонанс в обществе. Использование социальных сетей, видеохостингов, форумов и иных публичных ресурсов в сети Интернет, на которых террористы публикуют в открытом доступе материалы о проведенных ими терактах, значительно усиливает общественный резонанс, причем преступники, не связанные цензурой и самоограничениями, имеющими место в официальных средствах массовой информации, часто прибегают к дезинформации, в разы завышая причиненный ими ущерб.

Однако, несмотря на актуальность обозначенной проблемы, в рамках настоящей работы представляется правильным сосредоточиться на другом аспекте кибертерроризма – осуществлении террористических актов посредством компьютерных атак.

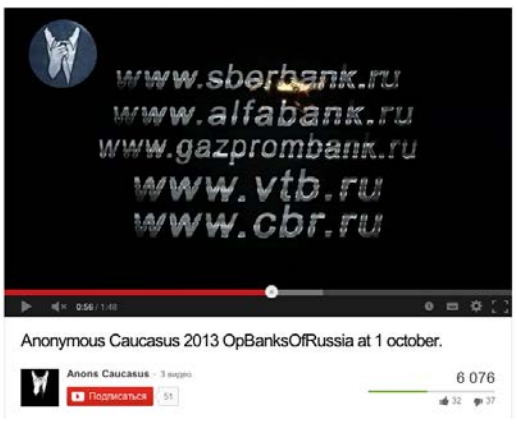
Еще в начале 2000-х гг. специалисты в сфере информационной безопасности дискутировали, достигли ли террористы уровня, который позволил бы им осуществить террористический акт, применив в качестве орудия совершения преступления вредоносную программу либо использовав уязвимости ПО. Сегодня такая дискуссия уже не актуальна, за последнее десятилетие было совершено несколько компьютерных атак, которые, несомненно, можно трактовать как кибертеррористические.

В октябре 2013 г. был совершен ряд *DDoS*-атак на сайты и сервисы нескольких российских банков. Незаконному воздействию последовательно подвергались сетевые ресурсы «Сбербанка России», банковской группы «Альфа-Банк», «Газпромбанка», банка ВТБ и ЦБ РФ.

Ответственность за произошедшее взяла некая группа, называющая себя «Электронная армия кавказского эмирата» (террористическая организация «Кавказский эмират» запрещена в России), которая 30 сентября 2013 г. опубликовала заявление о планируемых атаках на сайты российских банков в связи с ранее объявленной террористической организацией войной с Россией (*рис. 5.1–5.2*).

Атаки были осуществлены с использованием комплекса вредоносного ПО *Drive*, классифицируемого «Лабораторией Касперского» как *Trojan-DDoS*, который на тот момент предлагался к использова-

нию в формате партнерства на нескольких форумах киберкриминальной направленности.



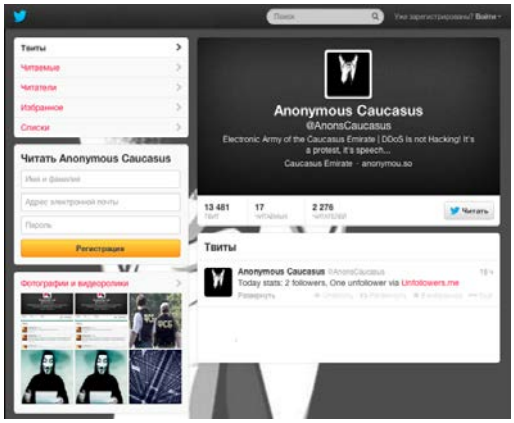


Рис. 5.1–5.2. Обращение группы, транслированное в видеоблоге и твиттере пользователя с сетевым псевдонимом *Anonymous Caucasus*

Drive DDoS Botnet System[1] является комплексом вредоносных программ, предназначенных для осуществления *DDoS*-атак посредством использования распределенных бот-сетей (*рис. 5.3*), созданных из компьютеров под управлением ОС *Windows*. Приведен географический состав бот-сети *Drive* (*рис. 5.4*).

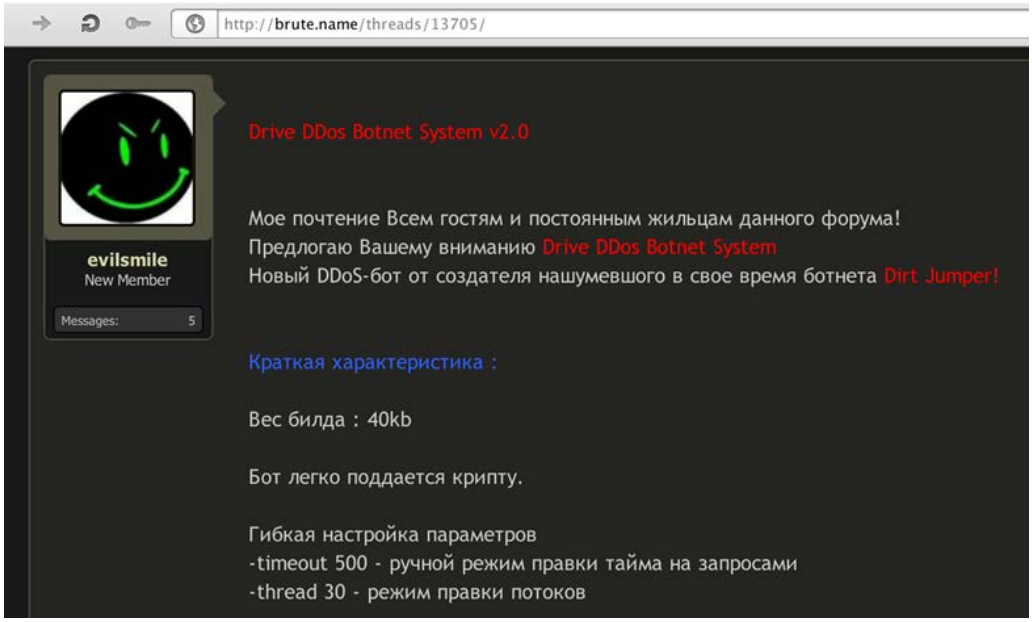


Рис. 5.3. Объявление о продаже вредоносной программы *Drive* на ресурсе киберкриминальной направленности *brute.name*

[1] Название и классификация, применяемые разработчиком.

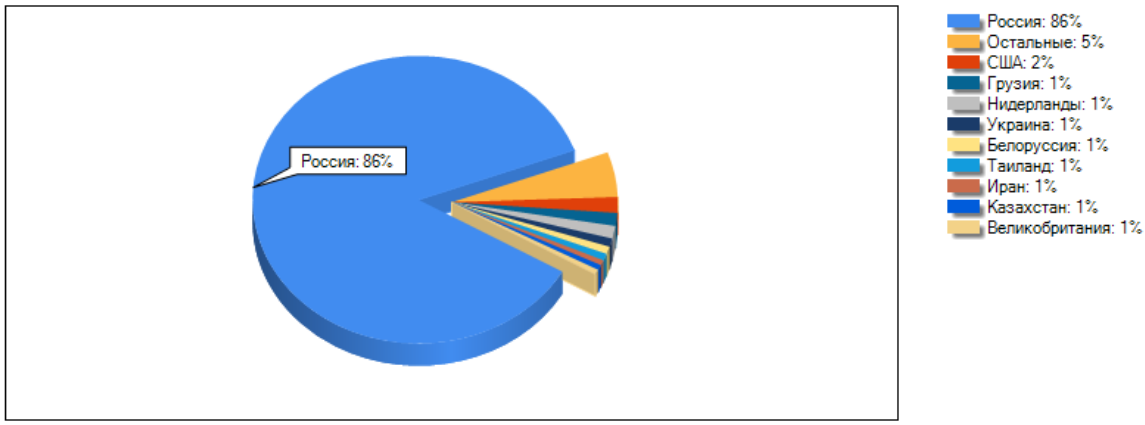


Рис. 5.4. Географический состав бот-сети *Drive* на момент атаки

Функционирование данного программного комплекса направлено на блокирование легальным пользователям доступа к какому-либо сайту и размещенной на нем информации, для чего используется воздействие на канал связи, который «забивается» огромной массой специально созданных запросов. Управление бот-сетью осуществляется с помощью веб-панели посредством передачи компьютерам-ботам команд о цели, начале и окончании атаки, ее типах, свойствах и применяемых средствах.

Последствия атак удалось минимизировать благодаря защитным мерам, своевременно принятым банковским сообществом совместно с компаниями, специализирующимися в области компьютерной безопасности, тем не менее преступные действия создали значительные затруднения в обеспечении штатного функционирования банковских ресурсов и потребовали проведения мероприятий, направленных на нейтрализацию угрозы.

Другая известная компьютерная атака, существенно повлиявшая на развитие ядерной программы Ирана и причинившая огромный ущерб, была совершена немногим ранее – в 2010 г.

Атака носила целевой многоступенчатый характер и была осуществлена с применением специально созданного компьютерного червя *Stuxnet* по сценарию, предполагавшему проникновение вредоносной программы в целевую инфраструктуру, не имеющую прямого подключения к глобальной сети Интернет, через цепочку сетевых ресурсов бизнес-партнеров.

Как установили исследователи вредоносного кода, он был написан высокопрофессиональной командой разработчиков, кроме того, ими были найдены следы применения в атаке весьма дорогих эксплойтов нулевого дня (*Zero-Day Exploit*), то есть эксплойтов, против

которых еще не разработаны механизмы защиты. Функциональные возможности вредоносной программы позволяют перехватывать и модифицировать данные, передаваемые между программируемыми контроллерами *Simatic* и системами *Simatic WinCC* компании *Siemens* таким образом, чтобы физически воздействовать на промышленную инфраструктуру. По оценке независимых исследователей, атака с применением червя *Stuxnet* нарушила работу более тысячи центрифуг на заводе по обогащению урана, а также сорвала сроки запуска АЭС в г. Бушере.

В какой-то момент атакующие утратили контроль над распространением вредоносной программы, в результате чего *Stuxnet* заразил сотни тысяч компьютеров по всему миру, не имеющих отношения к целевой системе (*рис. 5.5*).

Исследование вредоносного кода червя выявило следующие особенности:

– вредоносная программа имела цифровые подписи известных компаний – *Realtek* и *JMicron*, что позволяло ей избегать обнаружения антивирусным ПО, так как цифровые подписи служат признаком легальности программы;

– вредоносная программа распространялась через *USB*-флеш-накопители, эксплуатируя уязвимость ОС *Windows* в обработке ярлыков (*LNK*-файлов) с помощью эксплойта нулевого дня;

– вредоносная программа эксплуатировала еще две уязвимости ОС *Windows* с использованием эксплойтов нулевого дня, обеспечивающих функционирование червя путем повышения привилегий учетных записей, под которыми он был запущен, до уровня администратора системы.

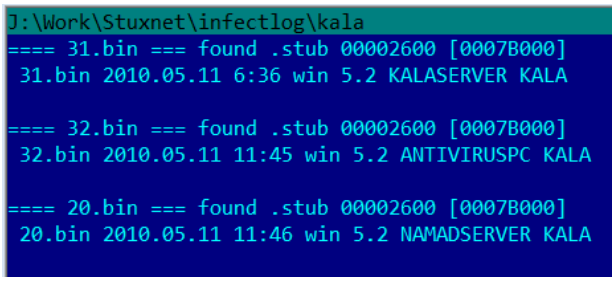


Рис. 5.5. Информация из трех разных файлов червя *Stuxnet* о зараженным им системах компании *Kala Electric*

Таким образом, сценарий атаки подразумевал поэтапное заражение бизнес-партнеров промышленных предприятий, работающих по реализации ядерной программы Ирана, компьютерные системы кото-

рых были изолированы от сети Интернет, с помощью *USB*-накопителей. Оказавшись в изолированных компьютерных системах, использующих программно-аппаратные решения *Simatic*, червь реализовал свое основное предназначение – воздействие на физическую инфраструктуру путем модификации компьютерной информации автоматизированных систем управления технологическими процессами (АСУ ТП).

В связи тем, что при заражении компьютеров червь *Stuxnet* сохраняет информацию об имени, домене и *IP*-адресе зараженной системы в своем файле и постоянно дополняет эту информацию новыми данными при распространении по сети, исследователям удалось выявить предприятия-партнеры, компьютерные системы которых были заражены червем на первом этапе атаки.

В результате анализа собранной информации было установлено, что атака началась не позднее июня 2009 г., некоторые из предприятий-партнеров подвергались заражению червем несколько раз со значительными временными интервалами, что свидетельствует об исключительной нацеленности атакующих на достижение результата – проникновение в изолированные промышленные системы.

Кроме того, исследователи с высокой степенью вероятности установили предприятие, с которого червь начал распространение по всему миру (*рис. 5.6*), а именно компанию *Behpajooh Co.* (*рис. 5.7*), специализирующуюся на разработке систем автоматизации промышленных производств.

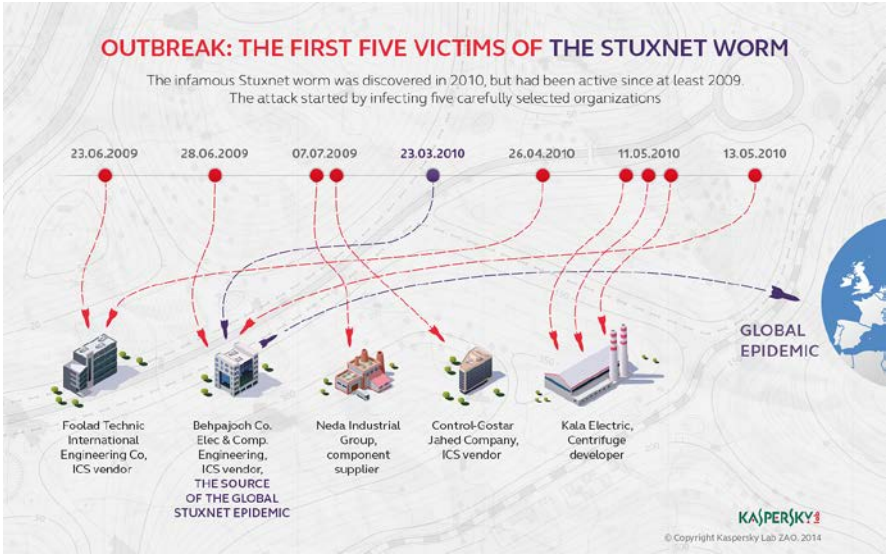


Рис. 5.6. Хронология заражений червем *Stuxnet* предприятий-партнеров

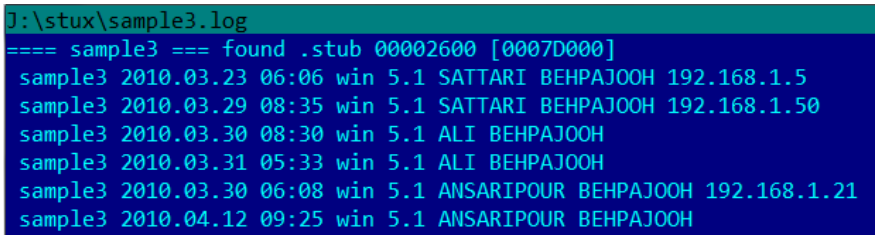


Рис. 5.7. Информация о заражениях червем *Stuxnet* устройств компании *Behpajooh Co*.

Факт изменения 29 марта 2010 г. сетевого адреса зараженного устройства, который отражен на рисунке, косвенно свидетельствует о том, что это был ноутбук, который периодически подключался в локальную сеть и мог являться источником дальнейшего распространения вредоносной программы.

История компьютерной атаки *Stuxnet* на промышленные предприятия, работавшие в рамках ядерной программы Ирана, является на сегодняшний день наиболее яркой иллюстрацией возможностей применения вредоносных программ в террористических целях.

Однако говорить о весьма высоком уровне кибертеррористической опасности приходится не только из-за самой возможности таких атак, но и доступности средств для их осуществления. В этом плане компьютерная атака *Stuxnet* является скорее исключением, поскольку на ее подготовку и осуществление затрачены значительные средства. Для совершения нападения достаточно и тех вредоносных программ, которые широко представлены на киберкриминальном рынке, как, например, уже упомянутые троянские программы для осуществления *DDoS*-атак либо программы-шифровальщики, или программы удаленного управления компьютерными системами. Оценивая сегодняшнее положение дел, приходится признать, что специалист в области информационных технологий, обладающий достаточно высоким уровнем профессиональных знаний и опытом, в состоянии получить несанкционированный доступ к инфраструктуре АСУ ТП, которая отнесена к критической информационной инфраструктуре, и совершить деструктивные действия и без применения вредоносных программ, используя только ошибки в организации мер безопасности и уязвимости программного и аппаратного обеспечения.

С целью выработки мер противодействия таким атакам «Лаборатория Касперского» проводит значительную по объему исследовательскую работу по выявлению потенциальных уязвимостей в критически важных инфраструктурах и промышленных системах, обеспечивающих жизнедеятельность людей в современном мире.

Исследовательская деятельность в этом направлении осуществляется в том числе и в формате проведения соревнований-учений, на которые приглашаются специалисты в области информационной безопасности АСУ ТП. Условия проведения учений максимально приближены к реальным, для чего создаются модели, имитирующие производственные площадки, например электрических подстанций, с использованием промышленного ПО и контроллеров предприятий. В рамках учений соревнующиеся команды в режиме реального времени атакуют как отдельные компоненты энергосистемы, так и архитектуру в целом.

Так, в г. Иннополисе Республики Татарстан в 2016 г. были проведены соревнования, в которых использовались модели генерации и потребления электроэнергии: ГЭС, солнечная станция, цифровая подстанция, город и завод.

В ходе учений менее чем за сутки одной из команд, использовавшей подключение к локальной сети, имитирующее доступ в сеть Интернет, удалось удаленно нарушить работу энергосистемы, спровоцировать короткое замыкание на электроподстанции, смоделировав локальное повреждение оборудования, и лишить таким образом потребителей источника энергии (*рис. 5.8*).

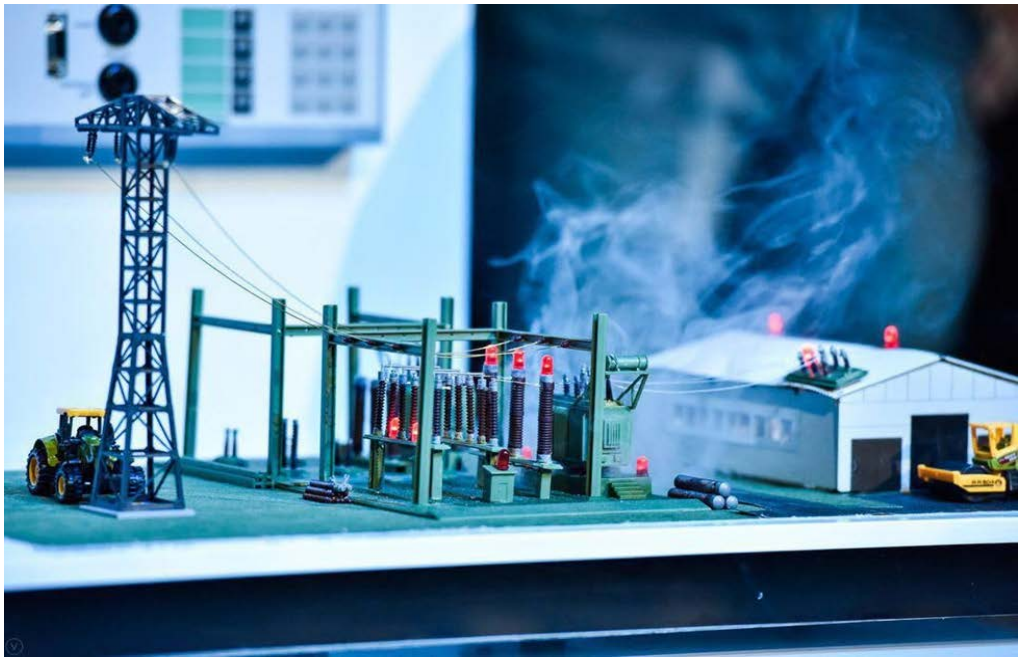


Рис. 5.8. Короткое замыкание на стенде модели электроподстанции

Рассмотрим более детально способ и механизм совершения возможной кибератаки на электроподстанцию на примере одного из этапов аналогичного соревнования, проводившегося на площадке форума по информационной безопасности *Positive Hack Days VI* в 2016 г.

В рамках учений была создана модель магистральной подстанции (*рис. 5.9*), имеющей классическую трехфазную архитектуру с резервированием, через которую с ГЭС осуществлялась поставка электроэнергии на распределительную подстанцию, обеспечивающую электричеством инфраструктуру небольшого поселка.

На мнемосхеме магистральной подстанции показан замкнутый контур из трех линий – две линии ввода (*W1* и *W2*) с выводом на трансформатор и одна межсекционная линия. Как видно из схемы, каждая линия оснащена силовым выключателем (*Q*), разъединителем (*QS*) и устройством заземления (*QSG*). Такая схема построения электросети подстанции позволяет быстро переключать нагрузку с основной линии на резервную и обратно (в случае возникновения аварии или ремонтных работ) без отключения источников и потребителей от электросети.

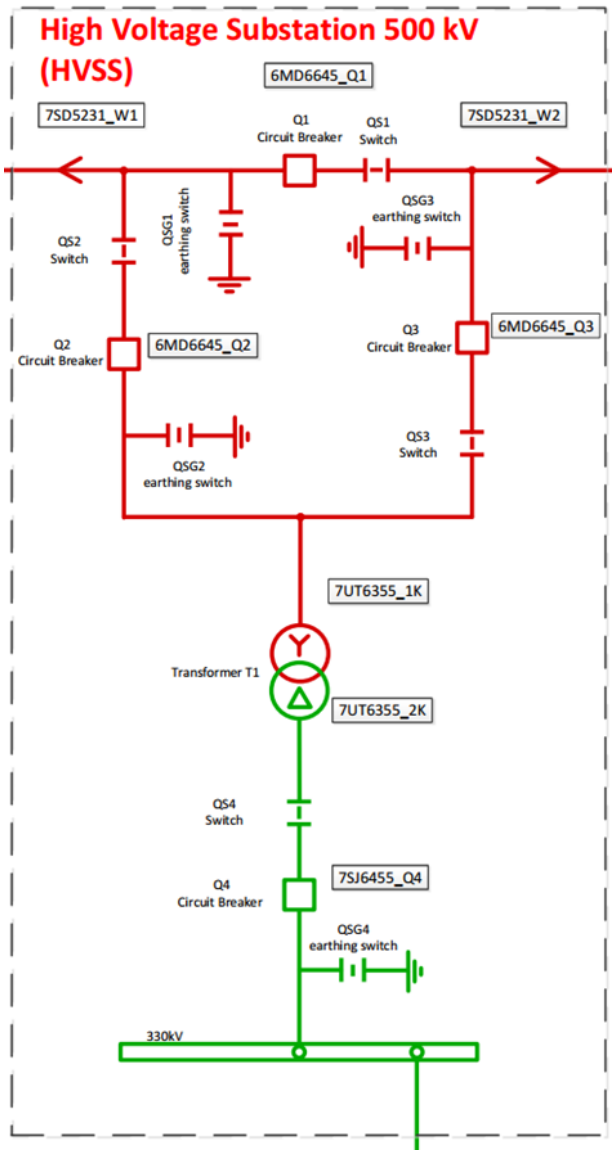


Рис. 5.9. Мнемосхема модели магистральной подстанции

На первом этапе атаки участники соревнования смогли подобрать пароль для подключения к веб-интерфейсу контроллера *Siemens S7-1500*. Дальнейший вектор атаки затрагивал промышленные протоколы передачи данных.

Получив доступ к терминалу релейной защиты и автоматики (РЗА), предназначенной для быстрого выявления и отключения поврежденных элементов электроэнергетической системы в аварийных ситуациях с целью обеспечения ее нормальной работы в целом, атакующие некоторое время тестировали возможные реакции системы на включения-выключения разъединителей *QS* и выключателей *Q*. В результате ими было установлено, что терминалы в автоматическом режиме управляют выключателями, разъединителями и заземляющими ножами, а в случае отсутствия явных признаков по-

вреждения оборудования, терминал РЗА той или иной линии переводил оборудование в режим резервирования, позволяющий быстро ввести линию в рабочий режим в случае отключения соседней линии (в результате аварии или ручного управления). Другими словами, терминалы РЗА магистральной подстанции были сконфигурированы на автоматическое резервирование линий электропередачи с целью непрерывного обеспечения потребителей электроэнергией. Изучив таким образом логику работы терминалов РЗА, участники соревнования начали массированную спуфинг-атаку (англ. *spoofing* – подмена) по промышленному протоколу *GOOSE* на терминалы линий 2 и 3. Спуфинг-атака заключается в том, что пользователь осуществляет рассылку сообщений, маскируясь под другого участника либо программу путем фальсификации данных, с целью получения неких преимуществ.

На протяжении 20 мин атакующий, заглушая настоящие сигналы системы, рассылал *GOOSE*-сообщения о том, что разъединители *QS2* и *QS3* выключены, то есть линии 2 и 3 обесточены (*рис. 5.10*).

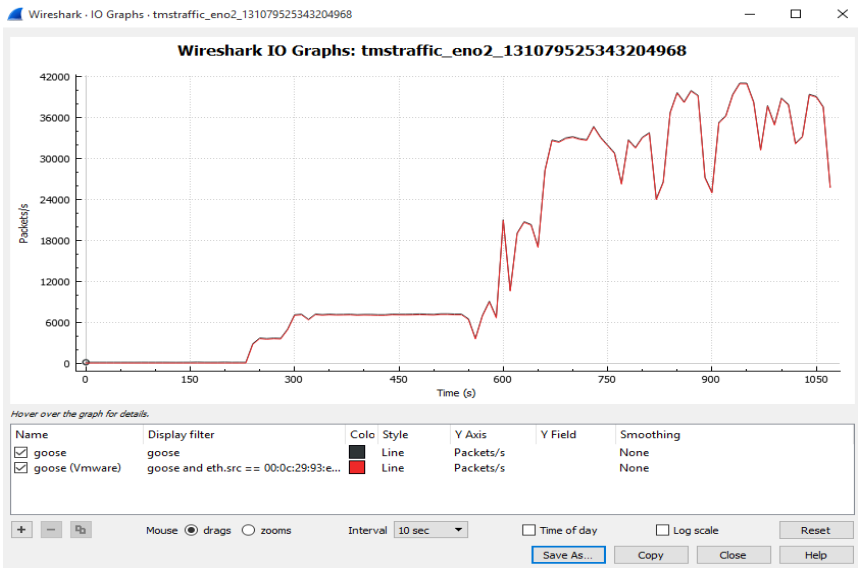


Рис. 5.10. Начало спуфинг-атаки на систему подстанции

После небольшой паузы атакующий отправил команду на включение заземляющих ножей (*QSG3*) на линии 3, находящейся в рабочем состоянии. Оперативные блокировки не сработали, поскольку терминал РЗА был уверен, что линия 3 отключена от сети, таким образом атакующему удалось спровоцировать короткое замыкание на линии 3 магистральной подстанции.

В момент возникновения короткого замыкания терминалы РЗА линий 1 и 3 оперативно отключили линию от сети, а терминал ли-

нии 2 подготовил линию к переходу в рабочий режим и перевел нагрузку, включив соответствующий силовой выключатель (*Q2*).

Моделирование дальнейшего развития событий показало, что ремонтная бригада устранила бы повреждение линии лишь спустя 4 часа. На время проведения ремонта магистральную подстанцию пришлось бы полностью обесточить, отключив выключатель на входной линии электропередачи, идущей от ГЭС, тем самым лишив поселок электроснабжения.

Анализ смоделированной ситуации позволяет сделать вывод, что для проведения подобных атак достаточно иметь познания в основах построения электросетей, устройстве терминалов релейной защиты и реализации промышленных протоколов.

Таким образом, детальное изучение потенциально возможной кибертеррористической атаки на промышленный объект демонстрирует, что для ее осуществления не требуется каких-то уникальных специальных познаний, а результаты ее совершения могут быть вполне сопоставимы с последствиями террористического акта в виде взрыва либо поджога.

Такие выводы выявляют еще одну проблему противодействия кибертерроризму, но в данном случае – уголовно-правового характера. Следственно-судебная практика рассматривает как проявление объективной стороны преступления, предусмотренного ст. 205 УК РФ, совершение взрыва или поджога либо иных сопоставимых действий, например распыления ядовитых химических веществ в общественном месте.

Между тем, согласно Инструкции по локализации и предупреждению взрывов пылегазовоздушных смесей в угольных шахтах, утвержденной приказом Ростехнадзора от 6 ноября 2012 г. № 634 (ред. от 22 июня 2016 г.) «Об утверждении Федеральных норм и правил в области промышленной безопасности», взрыв – это процесс выделения энергии за короткий промежуток времени, связанный с мгновенным физико-химическим изменением состояния вещества, приводящим к возникновению скачка давления или ударно-воздушной волны, сопровождающийся излучением и образованием сжатых газов или паров, способных производить работу.

Взрыв осуществляется посредством взрывного устройства, под которым в соответствии с постановлением Пленума Верховного Суда Российской Федерации от 12 марта 2002 г. № 5 (ред. от 3 декабря 2013 г.) «О судебной практике по делам о хищении, вымогатель-

стве и незаконном обороте оружия, боеприпасов, взрывчатых веществ и взрывных устройств» следует понимать промышленное или самодельное изделие, функционально объединяющее взрывчатое вещество и приспособление для инициирования взрыва (запал, взрыватель, детонатор и т. п.).

При этом смоделированная ситуация продемонстрировала, что короткое замыкание в результате компьютерной атаки хотя и не привело к разрушению объекта и не может рассматриваться ни как поджог, поскольку воспламенения не произошло, ни как взрыв, однако это повлекло бы отключение населенного пункта, в том числе больниц, детских образовательных учреждений, систем жизнеобеспечения и потенциально опасных технологических объектов, от электросети, что в реальных условиях может вызвать у населения панику и создать реальную угрозу жизни людей.

При таких обстоятельствах усматривается необходимость дополнения объективной стороны преступления, предусмотренного ст. 205 УК РФ, еще одним способом его совершения наряду со взрывом и поджогом – неправомерным воздействием на информационную инфраструктуру.

ГЛАВА 6. ОСОБЕННОСТИ СБОРА ДОКАЗАТЕЛЬСТВ ПО ДЕЛАМ О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ

6.1. Источники доказательств

Специфичные следы преступлений, орудия и средства их совершения в виде вредоносных и иных программ в основном могут быть обнаружены как структуры компьютерной информации, что обусловливает наличие присущих только им признаков. Несмотря на то, что для обнаружения, фиксации и изъятия компьютерных данных необходимо привлекать специалиста, следователю важно понимать, где искать компьютерную информацию, имеющую криминалистическое значение, каким образом произвести ее изъятие, какие свойства и характеристики вредоносной программы необходимо исследовать, чтобы в полной мере установить обстоятельства ее применения.

Помимо традиционных мест поиска следов преступления, которыми являются место нахождения преступника и место происшествия, следы преступлений в виде компьютерной информации могут быть обнаружены при передаче по каналам связи либо в месте хранения и автоматизированной обработки с использованием вычислительных мощностей:

– рабочее место преступника (компьютерные устройства, электронные носители информации, средства связи, записи);
– место происшествия (компьютерная система);
– сетевые ресурсы преступника (в локальной сети);
– сетевые ресурсы преступника (в глобальной сети);
– каналы связи преступника (сетевой трафик);
– легальные сетевые ресурсы, используемые в преступной деятельности (почтовые серверы, вычислительные мощности провайдеров хостинга, ресурсы провайдера по предоставлению доступа в сеть Интернет и т. п.).

Перечень электронно-вычислительной техники, которая может быть изъята в ходе обыска либо осмотра места происшествия:

– персональные компьютеры;
– ноутбуки, нетбуки и др.;
– серверы;
– смартфоны, телефоны;
– роутеры;
– внешние электронные носители;

– иные устройства (видеорегистраторы, игровые приставки и др.).

В случае выявления сетевых ресурсов в сети Интернет, используемых для осуществления преступной деятельности, источниками криминалистически значимой информации являются:

Провайдеры хостинговых услуг:

– журнальные файлы (лог-файлы) подключений к арендуемому сетевому ресурсу;

– цифровые копии содержимого серверов или облачных хранилищ информации.

Изучение лог-файлов подключений к серверу, использующемуся в киберкриминальной деятельности, позволяет обнаружить сетевые адреса пользователей этого ресурса и принять меры к установлению их личности. Если реальный *IP*-адрес пользователя скрыт прокси-сервером, необходимо при наличии возможности повторить эту операцию и попытаться проследовать по их цепочке.

В ходе исследования копий содержимого серверов могут быть подтверждены факты их использования при совершении киберпреступлений, обнаружены экземпляры распространяемых вредоносных программ, выявлены сетевые реквизиты пользователей: имена учетных записей и *IP*-адреса подключений, а также адреса других серверов сетевой инфраструктуры.

Провайдеры доступа в сеть Интернет:

– журнальные файлы доступа в сеть Интернет;

– статистические данные учета сетевого трафика.

Лог-файлы и статистические данные учета сетевого трафика, собираемые интернет-провайдерами, содержат сведения о сетевой активности пользователей конечных устройств, которыми могут быть как киберпреступники, так и потерпевшие в результате их деятельности. В любом случае информация может представлять интерес для следствия и быть использована для выявления сетевых адресов, с которыми конечные устройства взаимодействовали (серверы управления и распространения вредоносных программ, форумы киберкриминальной направленности, виртуальные обменные и платежные сервисы и т. п.).

При совершении хищений у пользователей-клиентов ДБО криминалистически значимые сведения содержатся в журнальных файлах серверной части интернет-банкинга. Интерес для следствия представляют *IP*-адреса подключений клиентов в ходе сессии, на протя-

жении которой были осуществлены несанкционированные финансовые операции. В случае если преступник формировал платежные документы на своем компьютере, может быть обнаружен его *IP*-адрес либо адрес используемого им прокси-сервера. Если хищение осуществлялось с использованием подставных юридических лиц, источником информации о лицах, фактически управляющих счетами этих предприятий, служат сведения об *IP*-адресах, с которых осуществлялись подключения к сервисам ДБО.

Существенные затруднения при определении источника, содержащего криминалистически значимую информацию, возникают при осмотре крупных компьютерных сетей, функционирование которых приостановить не представляется возможным в виду непрерывного производственного процесса. Кроме того, изъятие с места происшествия всей компьютерной сети с целью производства судебной экспертизы не является целесообразным и разумным, а в большинстве случаев – технически возможным. В этом случае перед следователем стоит задача на месте происшествия выявить компьютерные устройства, подлежащие изъятию. С целью оказания содействия следователю в поиске и обнаружении доказательств специалистом могут быть изучены следующие объекты и процессы на компьютерах сети.

Объекты и процессы для изучения:

- процессы выполняемых программ;
- планировщики задач ОС;
- сервисы ОС;
- сетевой трафик;
- файлы;
- журнальные файлы (лог-файлы).

Изучение активных процессов позволяет специалисту выявить подозрительные процессы, зачастую созданные как дочерние от системных, того же *explorer.exe*.

Изучение специалистом данных планировщика и сервисов позволяет выявить заражение, так как автозапуск вредоносного кода каждый раз при перезагрузке системы прописывается с помощью планировщика задач либо других средств.

Исследование сетевого трафика предоставляет специалисту возможность обнаружить следы вредоносной активности при обращении, например, вредоносной программы к управляющему серверу.

Еще одной меткой заражения являются характерные однотипные либо лексически схожие названия файлов конкретных вредоносных программ.

Лог-файлы ОС компьютеров и серверов локальной сети содержат различную информацию о событиях в системе, сетевых подключениях, авторизациях под конкретными учетными записями, удаленном запуске исполняемых файлов и т. п.

6.2. Следственные действия

Современным уголовно-процессуальным законодательством компьютерная информация как отдельный специфический вид доказательств не рассматривается, поэтому при ее обнаружении и фиксации необходимо руководствоваться общими правилами. В связи с этим следует подробно рассмотреть способы и приемы сбора доказательств, представленных в виде компьютерной информации, чтобы, с одной стороны, на практике избежать ошибок в процессуальном оформлении, а с другой – фактической фиксации с учетом их особенностей с другой, поскольку и те, и другие могут повлечь признание таких доказательств недопустимыми.

В настоящее время получение компьютерной информации, имеющей доказательственное значение, возможно в ходе следующих следственных действий:

- осмотр места происшествия;
- осмотр предметов, документов;
- следственный эксперимент;
- обыск;
- выемка.

Наиболее значимые мероприятия по сбору доказательств в виде компьютерной информации связаны с выездом на место, будь то доступ к рабочей станции подозреваемого в ходе обыска либо изъятие компьютерной техники потерпевших в процессе выемки, либо осмотр места происшествия – локальной компьютерной сети.

Следует обратить внимание, что изъятию подлежат все взаимосвязанные объекты, включающие в себя аппаратное, программное и информационное обеспечение и являющиеся составными частями единого информационного технологического процесса.

Данный вопрос наиболее актуален при выезде на место происшествия с целью осмотра скомпрометированной системы. Отсутствие

понимания, что и в каком виде изымать, насколько целесообразно детальное описание в протоколе подключений к скомпрометированному компьютеру периферийных устройств, в каких случаях в ходе осмотра необходимо произвести копирование компьютерной информации, в том числе создать посекторную копию жесткого диска *HDD/SSD*, приводит к неоправданному затягиванию и усложнению следственного действия. Рекомендации по обязательному описанию в любых ситуациях всех соединений осматриваемого компьютера, маркировке всех портов и разъемов, кабелей, плат расширения и других подключенных устройств не всегда оправданны. Выполнение большого количества формальных и рутинных действий, которые никоим образом не влияют ни на качество изымаемых доказательств, ни на полноту последующего экспертного исследования, может повлечь существенные ошибки как процессуального, так и технического характера. Еще более эта проблема усугубляется, когда вся изъятая таким образом вычислительная техника (системные блоки, мониторы, принтеры, кабели, расширительные платы, *USB*-накопители и т. п.) направляется на судебную компьютерную экспертизу на предмет обнаружения и исследования программ, обладающих признаками вредоносности. По существу, на эксперта возлагается обязанность по осмотру всех изъятых устройств, даже если они не имеют отношения к исследованию. Представляется, что в таком сложном мероприятии, как осмотр компьютерных систем и их сетей, проводимый с целью обнаружения и изъятия криминалистически значимой компьютерной информации, любые действия должны быть разумны и обоснованны.

Детальное описание устройств, их маркировка и схема подключения, несомненно, требуются, если они являются составными частями единого скомпрометированного информационного технологического процесса.

Например, при хищении денежных средств в электронных платежных системах необходимо зафиксировать подключение к скомпрометированному компьютеру аппаратного токена. А в случае осмотра аппаратно-программного комплекса, к которому подключены специальные вычислительные модули, предназначенные для осуществления *DDoS*-атак, подробное описание всей системы и схемы подключений позволит эксперту воссоздать систему с целью исследования ее свойств.

Объем производимых действий, направленных на обнаружение и закрепление криминалистически значимой информации, необходимо

определять с участием специалиста, область специальных познаний которого должна быть достаточно широка: в сфере компьютерных устройств и программирования, в области сетевого взаимодействия и эксплуатации сетевой инфраструктуры и т. п. В исключительных случаях следует привлекать для производства таких мероприятий нескольких специалистов с углубленными познаниями в определенных областях компьютерно-информационных технологий.

Журнальные файлы доступа к ресурсам и копии содержимого серверов либо облачных хранилищ информации предоставляются провайдерами соответствующих услуг на электронных носителях информации, изъятие которых целесообразно производить в рамках выемки. Необходимо обратить внимание: если изымаемые сведения содержат государственную или иную охраняемую законом тайну, такие как личная переписка на почтовом сервере, требуется судебное разрешение на производство выемки.

В некоторых случаях получение информации с публичных веб-ресурсов, например в виде *HTML*-страниц, возможно оформить в рамках осмотра электронного документа с применением технического средства – компьютера, подключенного к сети Интернет. Но в основном в рамках следственных действий, предусмотренных действующим законодательством, способы и методы удаленного получения компьютерной информации с каналов связи и компьютерных систем процессуально реализовать не представляется возможным.

Распространенным следственным действием по делам о хищениях в электронных платежных системах является допрос. Особое значение имеет допрос потерпевших и очевидцев происшествия на первоначальной стадии расследования, когда выявлен факт несанкционированной денежной операции, но механизм совершения преступления не установлен. Показания свидетелей и потерпевших оказывают существенную помощь в скорейшем установлении способа совершения преступления, выявлении компьютеров, задействованных в манипулировании компьютерной информацией с целью хищения либо распространения вредоносных программ внутри локальной сети, определении времени заражения вредоносными программами и получения несанкционированного доступа. Показания в этой части важны не только для правильного планирования и качественного осмотра места происшествия, но и при производстве судебной компьютерной экспертизы.

Судебные экспертизы по делам о преступлениях в сфере компьютерной информации имеют чрезвычайно важное значение. При расследовании так называемых традиционных видов преступлений следы их совершения бывают достаточно явными, доступными для визуального осмотра либо выявляемыми распространенными криминалистическими методами и средствами. Киберпреступления представляют собой иной случай. Компьютерная информация, которая подверглась неправомерному воздействию, может быть обнаружена, осмотрена и исследована только опосредованно с применением компьютеров и специальных криминалистических программ, никаким иным способом установить обстоятельства совершенного преступления невозможно. При таких обстоятельствах роль судебного эксперта в установлении истины по делу становится одной из ведущих.

6.3. Использование в доказывании результатов оперативно-разыскной деятельности

Уголовно-процессуальное законодательство Российской Федерации допускает использование результатов, полученных в ходе проведения оперативно-разыскных мероприятий, если они отвечают требованиям, предъявляемым к доказательствам.

Согласно положениям ст. 11 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», результаты такой деятельности могут быть использованы для подготовки и осуществления следственных и судебных действий, проведения оперативно-разыскных мероприятий по выявлению, предупреждению, пресечению и раскрытию преступлений, выявлению и установлению лиц, их подготавливающих, совершающих или совершивших.

Результаты оперативно-разыскной деятельности могут служить поводом и основанием для возбуждения уголовного дела, представляться в орган дознания, следователю или в суд, в производстве которого находится уголовное дело или материалы проверки сообщения о преступлении, а также использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства Российской Федерации, регламентирующими собирание, проверку и оценку доказательств.

Законом предусмотрены как специальные мероприятия – снятие информации с технических каналов связи и получение компьютерной информации, так и иные мероприятия, в ходе которых может быть произведен поиск, обнаружение и изъятие компьютерных данных.

Оперативно-разыскные мероприятия:

– сбор образцов для исследования;
– снятие информации с технических каналов связи;
– получение компьютерной информации;
– исследование;
– оперативный эксперимент.

При этом необходимо отметить, что удаленное получение (снятие) компьютерной информации представляет исключительно важное значение в доказывании при расследовании киберпреступлений, документировании преступной деятельности и установлении лиц, ее осуществляющих.

Вследствие того, что киберпреступники уделяют особое внимание мерам конспирации, изъятие у провайдеров хостинговых услуг копий содержимого серверов, задействованных в преступной деятельности, может не принести результата. Для создания копии сервера провайдеру необходимо выключить систему, однако на выключенной машине данные хранятся в зашифрованном виде с помощью специализированных программ (например, *TrueCrypt*). Для того, чтобы получить доступ к информации, содержащейся на изъятой копии сервера, необходимо ввести пароль либо использовать криптографический ключ, которыми следствие в большинстве случаев не располагает. Другой способ получения доступа к информации, имеющей значение для дела, – произвести удаленное подключение к серверу в процессе его работы, который может быть реализован в рамках проведения оперативно-разыскных мероприятий по поручению следователя.

Полученная компьютерная информация с прокси-серверов содержит сведения об адресах серверов управления в конфигурационных файлах настройки, журнальные файлы сетевых подключений, среди которых могут быть сетевые адреса участников преступной группы, осуществляющих настройку и администрирование сервера, а также сетевые адреса компьютеров пользователей, зараженных вредоносной программой, которая через прокси-сервер осуществляет взаимодействие с сервером управления.

Еще более значимым для расследования уголовного дела является мероприятие, связанное с получением компьютерной информации непосредственно с сервера управления, с помощью которого осуществляется основной объем преступных действий, в том числе от-

даются команды на совершение несанкционированных финансовых операций. В зависимости от конкретных обстоятельств данное мероприятие может проводиться разово либо в режиме мониторинга. Полученная компьютерная информация может содержать сведения об использовании сервера для несанкционированного доступа к компьютерам пользователей, о наличии на нем вредоносных программ и их функциональных возможностях, о сетевых адресах, с которых осуществляется управление сервером, о совершенных с применением сервера хищениях в электронных платежных системах и др.

Таким образом, проблемные ситуации, вызванные тем, что уголовно-процессуальным законом не предусмотрены следственные действия по получению компьютерной информации с удаленных компьютерных систем и их сетей, могут быть разрешены посредством поручения производства таких мероприятий органу, осуществляющему оперативно-разыскную деятельность.

6.4. Требования к специалисту, привлекаемому к сбору доказательств

Действующим законодательством не предусмотрено специальных регламентов следственных действий, учитывающих особенности обнаружения и фиксации доказательств в виде компьютерной информации, если не считать обязательного привлечения специалиста к изъятию электронных носителей информации в случаях, предусмотренных ч. 2 ст. 164.1 УПК РФ. Сами по себе эти требования не разрешают рассматриваемую проблему, а зачастую, напротив, усложняют проводимые мероприятия, так как, с одной стороны, для изъятия электронного носителя информации в виде *USB*-флеш-накопителя либо оптического диска какой-то особой технической подготовки не требуется, а с другой – предусмотренное этой же статьей обязательное присутствие понятых при изъятии компьютерной информации с работающей системы нецелесообразно и крайне затруднительно, учитывая длительность мероприятия и отсутствие у понятых специальных знаний. При этом следует учитывать, что для не обладающего специальными познаниями человека процесс осмотра специалистом вычислительной техники, связанной с обнаружением и копированием компьютерной информации, сравним с производством сложной судебной экспертизы.

В связи с изложенным, помимо удостоверения понятыми факта и результатов мероприятия необходимо предусмотреть и другие спо-

собы проверки достоверности изъятой компьютерной информации и допустимости примененных специалистом средств и методов, которые будут рассмотрены в следующей главе.

Привлечение специалиста к проведению следственных действий по уголовным делам о преступлениях в сфере компьютерной информации требует от следователя понимания, каким требованиям должен соответствовать специалист, какими методиками обладать, какими средствами компьютерной криминалистики владеть, чтобы обеспечить исчерпывающие меры к обнаружению и фиксации доказательств и исключить их утрату.

Требования к специалисту:

– опыт администрирования компьютеров под управлением различных ОС (*Windows, Linux, MacOS, iOS, Android* и т. д.);

– познания в сфере сетевых технологий (локальных и глобальной сетей, сетевого оборудования, сетевых протоколов);

– навыки обратной разработки (реверс-инжиниринга) и исследования вредоносного кода;

– владение методами компьютерной криминалистики;

– осведомленность в правоприменительной практике и в криминальных тенденциях в сфере компьютерной информации.

Ни один перечень оборудования, инструментов и ПО, которые могут быть востребованы специалистом при изъятии компьютерной техники, обнаружении, осмотре и фиксации компьютерной информации, не может считаться исчерпывающим и должен составляться исходя из конкретных обстоятельств дела. Можно лишь говорить о необходимом минимуме, список которого приведен на схеме ниже.

Инструменты, необходимые специалисту для осмотра:

– программы для снятия снимка (дампа) оперативной памяти (например, *Belkasoft RAM Capturer*, *ProcDump*);

– устройства, позволяющие изучать содержимое файловой системы в режиме «только чтение»;

– устройства-блокираторы для копирования *HDD*/*SSD*, исключающие возможность внесения изменений в исходный диск.

Участие специалиста в расследовании компьютерных преступлений имеет еще один специфический аспект, связанный с тем, что компьютерные данные очень легко уничтожить либо зашифровать, чем пользуются киберпреступники, чтобы скрыть доказательства от следствия. С учетом этого роль специалиста – не только оказать со-

действие в поиске и обнаружении доказательств и применении технических средств, но и обеспечить доступ к компьютерной информации, имеющей значение для дела. Поэтому крайне важно привлекать специалиста на этапе планирования и подготовки следственных действий, связанных с поиском, обнаружением и изъятием компьютерных данных, чтобы он мог дать компетентные разъяснения относительно доступности электронных доказательств и необходимости принятия мер к их сохранности.

6.5. Проблемы сбора доказательств на современном этапе

Проблемные ситуации, с которыми сталкивается следователь в процессе сбора доказательств по делам о преступлениях в сфере компьютерной информации, возникают довольно часто и бывают вызваны как объективными причинами, объяснимыми самой природой компьютерных данных, так и субъективными, связанными с недостатками организационно-методического, правового и образовательного плана.

Под компьютерной информацией, по смыслу примечания к ст. 273 УК РФ, понимаются цифровые данные, представленные в формализованном виде, пригодном для хранения на электронных носителях, обработки компьютерами и передачи по их сетям.

В этом плане можно говорить об электронных цифровых следах, которые обладают только им присущими свойствами:

– существуют в виде компьютерной информации;

– характеризуются высокой скоростью трансформации;

– отличаются невозможностью восприятия непосредственно органами чувств, а только с помощью специальных устройств и программ;

– требуют новых, отличных от традиционных способов, методов и процедур по обнаружению, фиксации и обеспечению сохранности;

– подтверждаются контрольными суммами либо иными данными, свидетельствующими об их целостности.

Учитывая, что такие данные могут быть представлены практически бесконечным количеством копий, легко распространены в компьютерных сетях и быть доступны в любой точке мира, где имеется подключение к сети Интернет, очевидно, что их природа кардинально отличается от представления традиционных овеществленных следов. Однако уголовно-процессуальным законом цифровые следы как особый вид доказательств не рассматриваются, что значительно услож-

няет процесс их сбора и фиксации. Сами по себе электронные цифровые следы могут быть приобщены к материалам уголовного дела только на носителе информации, но изъятие ее может быть произведено без привязки к какому-либо материальному носителю. Например, при получении компьютерной информации из компьютерной сети путем перехвата сетевого трафика либо с работающей компьютерной системы. Конечно, полученная информация будет законсервирована на электронном носителе информации, имеющем серийный номер и маркировку производителя, но идентичность полученной копии информации ее оригиналу будет подтверждаться другими характерными признаками: контрольной суммой (хеш-суммой), рассчитанной по криптографическому алгоритму, размером файла и другими его атрибутами. Таким образом, при работе с электронными цифровыми следами следователь должен относиться к процессу их изъятия с особым вниманием и тщательностью, не допуская отступлений от формального порядка протоколирования индивидуальных признаков и особенностей электронного носителя информации, используемого для консервации компьютерных данных, и одновременно фиксируя характеристики электронных следов как нового, но не регламентированного уголовно-процессуальным законом вида доказательств.

Вследствие этого до настоящего времени не разработаны отличающиеся полнотой криминалистические методики по поиску, обнаружению, фиксации и исследованию электронных цифровых доказательств, не составлен перечень рекомендуемых, а возможно сертифицированных аппаратных и программных средств компьютерной криминалистики, не проявляется явно существующая необходимость дополнения уголовно-процессуального закона новыми следственными действиями, регламентирующими способы и процедуры получения криминалистически значимой компьютерной информации.

Указанные обстоятельства значительно осложняют для следствия и суда оценку доказательств по делам о преступлениях в сфере компьютерной информации с точки зрения относимости, допустимости и достоверности.

Другие проблемы поиска, обнаружения, фиксации и изъятия электронных цифровых следов обусловлены природой их представления в виде компьютерной информации.

Обращение компьютерной информации в сети Интернет носит трансграничный характер. Неправомерное воздействие на компью-

терную информацию, хранящуюся и обрабатываемую компьютерными системами на территории Российской Федерации, может осуществлять вредоносная программа, сервер управления которой скрыт прокси-серверами, расположенными в юрисдикции других государств. Для выявления адреса управляющего сервера необходимо направить международные запросы об оказании правовой помощи в изъятии у провайдеров хостинговых услуг сведений о сетевых соединениях прокси-серверов и копий их содержимого. С учетом времени на подготовку и направление международного запроса его исполнение заведомо не принесет результата, поскольку за этот период произойдет неоднократная смена прокси-серверов.

Компьютерная информация характеризуется высокой скоростью трансформации: по своей природе электронные цифровые данные легко уничтожить и модифицировать. В связи с этим даже незначительное промедление с фиксацией обнаруженных цифровых следов может повлечь их утрату.

ГЛАВА 7. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА НЕКОТОРЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

7.1. Общие принципы работы с электронными доказательствами

При работе с электронными цифровыми данными помимо следования процессуальному порядку важно соблюдать и определенные правила компьютерной криминалистики.

Основные правила работы с цифровыми данными:

– неизменность компьютерной информации, хранящейся на изымаемых или осматриваемых устройствах;

– привлечение специалиста, имеющего соответствующую подготовку, для изъятия и (или) изучения компьютерной информации на изымаемых или осматриваемых устройствах;

– обязательность документирования в полном объеме действий по изъятию, хранению, передаче компьютерной информации и доступу к ней и, соответственно, к устройствам, на которых она содержится, обеспечение ее защиты и доступности для исследования.

Если в ходе следственного действия возникла необходимость в доступе к работающей компьютерной системе, следует запротоколировать все действия специалиста и используемые им оборудование и ПО, чтобы при последующей экспертизе были понятны и объяснимы любые изменения компьютерной информации, внесенные в результате доступа. По возможности доступ к электронно-вычислительному устройству осуществлять в режиме «только чтение».

Перед выездом необходимо использовать все имеющиеся возможности для предварительного получения информации о месте производства следственного действия, установленном оборудовании и программных средствах. Если выезд связан с осмотром места происшествия, существенное значение имеют сведения о дате и времени совершения преступления, местонахождении скомпрометированного компьютера, модели и характеристиках компьютера и его жесткого диска *HDD/SSD*, сетевом окружении и т. п. Помимо этого, на стадии подготовки к выезду на место происшествия следует согласовать участие в осмотре компьютера его владельца (физического лица либо руководителя предприятия, бухгалтера), непосредственного пользователя, а также системного администратора, которого следует поставить в известность о необходимости подготовить дополнительные сведения: журналы сетевой активности, а при наличии – журналы систем обнаружения вторжения, которые подлежат изъятию.

Вопросы, связанные с фиксацией обнаруженной компьютерной информации и упаковкой электронных носителей, на которых данная информация законсервирована, требуют некоторых пояснений. Общие криминалистические рекомендации в основном содержат требования к обеспечению сохранности и механической целостности изъятых устройств, предотвращению несанкционированного доступа к устройствам. При этом в протоколе должны быть зафиксированы индивидуальные признаки изъятых устройств и электронных носителей информации, позволяющие идентифицировать их и, соответственно, хранящуюся на них компьютерную информацию. Такие общие требования по отношению к компьютерной информации нельзя признать достаточными для обеспечения ее сохранности и дальнейшей идентификации. Выше уже рассматривались признаки компьютерной информации как специфического вида доказательств, в том числе отсутствие строгой структурированности, скорость модификации, невосприимчивость органами чувств человека, идентификация по хеш-сумме. Нередки случаи, когда криминалистически значимая компьютерная информация копируется в виде файлов и папок с рабочей («живой») системы либо с удаленного ресурса. Очевидно, что какими-либо внешними характерными признаками они не обладают, если не считать таковыми свойства в виде размера либо вида файлов, но такие свойства имеют слишком общий характер. Именно с помощью вычисления хеш-суммы (контрольной суммы) по определенному алгоритму (*MD5, SHA256* и т. п.) и возможно на любом этапе расследования подтвердить идентичность исследуемой компьютерной информации изъятой. Сведения о хеш-сумме изъятой компьютерной информации вносятся в протокол. В данном случае даже повреждение электронного носителя, на который была скопирована изъятая информация, не повлечет ее утраты, если она была сохранена на других устройствах. Доказательство будет восстановлено путем копирования на новый электронный носитель, а его достоверность подтверждена хеш-суммой. Таким образом, хотя с процессуальной точки зрения доказательствами являются электронный носитель информации, а также протокол его осмотра, по существу, в качестве доказательства можно рассматривать компьютерную информацию, обладающую только ей присущими признаками и свойствами и законсервированную на электронном носителе. Еще одна ситуация, демонстрирующая специфичность осмотра и выемки компьютерной техники с хранящейся на ней криминалистически значимой информацией, может возникнуть при изъятии авто-

номных устройств (ноутбуков, смартфонов), экран которых заблокирован, но сами они находятся во включенном состоянии. При наличии доступа к сети Интернет, например по стандартам передачи данных в сотовых сетях, возможно удаленное подключение к ним посторонних лиц и внесение изменений в хранящуюся на них компьютерную информацию. То есть в этом случае, несмотря на формальное соблюдение всех процессуальных требований по изъятию компьютерной техники, не обеспечена целостность и неизменность хранящейся на ней компьютерной информации.

7.2. Осмотр места происшествия

Осмотр места происшествия при расследовании уголовных дел о преступлениях в сфере компьютерной информации сочетает в себе действия как направленные для поиска традиционных вещественных следов преступления, так и для обнаружения и фиксации электронных цифровых следов. Представляется целесообразным сосредоточиться на особенностях и следственных ситуациях, связанных с поиском, обнаружением и изъятием компьютерной информации, поскольку работа с традиционными следами затруднений не вызывает. Вместе с тем необходимо отметить, что при проведении осмотра места происшествия следователь должен рассматривать версию о совершении преступления, связанного с несанкционированным воздействием на компьютерную информацию, работником пострадавшей организации. По мере установления обстоятельств преступного посягательства и выявления вовлеченных в его совершение компьютерных систем, следователь, в зависимости от конкретной ситуации, обязан предпринять меры по обнаружению и фиксации традиционных следов – следов взлома в помещение с ограниченным доступом – серверную, отпечатков рук на клавиатуре и корпусе компьютерных терминалов, изъятию записей с камер видеонаблюдения и т. п. В то же время осмотр компьютерной информации также должен производиться с учетом следственной версии об инсайдере.

Общий порядок действий при осмотре компьютерной техники:

– внешний осмотр компьютерной техники;

– осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов);

– снятие копии (дампа) содержимого оперативной памяти;

– переключение в режим гибернации (отметить в протоколе);

– отсоединение кабелей и внешних устройств (в случае изъятия взаимосвязанных объектов предварительно отметить, к какому порту что подключено);

– создание копии жесткого диска *HDD/SSD* (в случае необходимости);

– упаковка изъятого.

Этапы осмотра и типичные ситуации.

Осмотр включенного персонального компьютера, ноутбука, нетбука:

1. Внешний осмотр (фирма-производитель, модель; подключенные кабели, в том числе сетевые; подключенные внешние электронные носители и устройства; наличие либо отсутствие оптических дисков в приводах и иных электронных носителей в соответствующих устройствах ввода-вывода; состояние, внешние дефекты, комплектность).

2. Осмотр компьютерной информации (признаки, свидетельствующие об использовании компьютера при совершении киберпреступлений):

а) выявление специфического ПО:

– программ, обеспечивающих шифрование файлов;

– программ для создания и использования криптоконтейнеров;

– программ, обеспечивающих функционирование виртуальных машин;

– программ-менеджеров паролей;

– программ-клиентов мгновенного обмена сообщениями, поддерживающих шифрование трафика;

– программ для написания приложений – среды разработки;

– специфических утилит (программы-спамеры и т. п.);

б) изучение файловой системы:

– исследование логической структуры дисков на предмет выявления неразмеченной области большого размера;

– исследование файловой системы на предмет обнаружения файлов больших размеров, возможно являющихся криптоконтейнерами;

– визуальный осмотр рабочего стола на предмет выявления следов противоправной деятельности.

3. Изучение процессов, запущенных на компьютере.

4. Снятие копии (дампа) содержимого оперативной памяти.

В случае если на момент осмотра компьютер выключен, но оперативная необходимость требует предварительного осмотра содержащейся в нем информации, следует сначала создать копию *HDD/SSD*, а затем провести осмотр, загрузив систему с копии. Оригинальный *HDD/SSD* изымается.

В некоторых случаях достаточно создать копию лишь шифруемой области компьютерных данных (так называемых криптоконтейнеров), чтобы провести их оперативный осмотр, а не всего *HDD/SSD*.

Если криминалист ограничен в возможностях изъять устройство и изготовить полную копию диска вследствие его большого размера (например, при осмотре сервера, изъятие которого из рабочего процесса может повлечь критические последствия), доступны следующие варианты действий:

1) создание копии логического (а не физического) диска в случае, если размер логического диска несопоставимо меньше неразмеченной области физического диска, например с помощью специальной криминалистической программы – *EnCase Forensic Imager*;

2) целевое копирование файлов, если известны сведения, представляющие интерес, и их расположение в файловой системе осматриваемого устройства; требование при копировании – рассчитать хеш-сумму скопированных файлов и внести в протокол – оптимально создать архив на осматриваемом устройстве, содержащий все имеющие значение для следствия файлы, вычислить его сумму, потом скопировать и подтвердить идентичность копии проверкой хеш-суммы;

3) копирование файлов и получение иной информации, содержащих достаточно сведений для оперативного анализа о возможной компрометации устройства либо его использовании в противоправных целях, таких как:

- копия (дамп) содержимого оперативной памяти;
- файл гибернации;
- страничный файл;
- ветви реестра ОС;
- журнальные файлы;
- файл *$MFT* (*Master File Table*);
- файл *Prefetch*;
- файл-листинг с хеш-суммами;

а также в конкретных случаях:

– файлы, содержащие копии веб-страниц, посещенных с помощью браузеров;

– файлы, содержащие историю посещения веб-страниц;

– архив электронной почты;

– настройки *VPN*;

– профили пользователей и т. п.

Ниже схематично и упрощенно изложен порядок действий при осмотре компьютерной техники при выезде на место происшествия.

Обязательные действия:

– проверка наличия активных сетевых подключений;

– отключение сетевых подключений (извлечение сетевого кабеля);

– получение снимка (дампа) содержимого оперативной памяти;

– выключение компьютера и создание копии жесткого диска;

– составление протокола и упаковка изъятого.

Осмотр компьютерной техники (факультативные действия):

– выявление определенного ПО (среды разработки; специфических утилит, например сканеров портов; программ для шифрования дисков, папок и файлов; виртуальных машин; менеджеров паролей и т. п.);

– исследование файловой системы и логической структуры дисков на предмет обнаружения области, где могут быть скрыты зашифрованные данные, а также файлов больших размеров, которые, возможно, являются криптоконтейнерами;

– изучение активных процессов на предмет выявления подозрительных.

7.3. Производство обыска

Действия, направленные на поиск, обнаружение и фиксацию компьютерной информации при проведении обыска, во многом схожи с аналогичными действиями в ходе осмотра места происшествия, производящегося с учетом следственной версии о возможном участии в преступлении работника пострадавшей организации. Однако существенное значение имеют тактические особенности производства обыска по уголовным делам о компьютерных преступлениях.

Лица, осуществляющие противоправные действия в сфере компьютерной информации, активно пользуются различными средствами и способами, обеспечивающими конспиративность их деятельности:

шифрованием данных, выходом в сеть Интернет с помощью анонимайзеров (ресурсов, скрывающих *IP*-адрес), программами для безвозвратного удаления данных и т. п. При таких обстоятельствах зафиксировать и сохранить интересующую информацию возможно только на «живой», то есть настроенной и работающей ОС. В связи с этим основными требованиями, которые должны учитываться при подготовке к мероприятиям по обнаружению и изъятию значимой компьютерной информации у подозреваемых лиц, являются: а) использование фактора неожиданности; б) своевременность проникновения в помещение. Необходимо получить доступ к работающему устройству и пресечь попытки подозреваемого уничтожить хранящуюся на нем информацию путем применения специальных программ либо выключения системы. Для этого представляется целесообразным на стадии подготовки к обыску дать поручение органу, осуществляющему оперативно-разыскную деятельность, о сборе сведений о распорядке дня подозреваемого, запорных устройствах и замках входной двери в помещение, где планируется обыск, мониторинге сетевой активности с помощью контроля интернет-канала подозреваемого с целью определения времени проникновения в помещение. Однако необходимо учитывать, что подозреваемый, соблюдая меры конспирации, может использовать не личный проводной интернет-канал, а *Wi-Fi*-роутер, расположенный поблизости, к которому у него имеется возможность несанкционированного подключения. В этом случае важно не допустить следственной ошибки, чтобы не провести обыск у не имеющего отношения к преступной деятельности лица, при том что информация об этом станет известна подозреваемому.

Тактические особенности производства обыска:

– пресечь доступ подозреваемому к компьютерной технике, исключить возможность использования им средств, предназначенных для уничтожения информации;

– предпринять меры к предотвращению блокировки работающих компьютеров по тайм-ауту;

– произвести фотографирование отображаемого на экранах компьютеров;

– проверить наличие активных сетевых подключений, исключить возможность удаленного доступа к управлению изымаемой компьютерной техникой со стороны соучастников;

– сделать снимок (дамп) содержимого оперативной памяти;

– произвести копирование файлов из открытых криптоконтейнеров на внешний носитель;

– проверить признаки использования удаленных серверов для хранения информации (облачных хранилищ), скопировать данные при наличии активных подключений.

Эффективность обыска в существенной мере зависит от понимания, поиск какого предмета или информации проводится. В зависимости от преступной роли и возложенных на них в преступной группе обязанностей у подозреваемых лиц могут храниться предметы и информация, перечисленные на схеме.

Тактические особенности производства обыска у участников преступной группы:

– у организаторов и руководителей группы: на компьютере – клиенты обмена сообщениями, контактные листы, история переписки, финансовые документы;

– у разработчиков программного обеспечения, или крипторов: на компьютере – исходные коды, среда разработки, скомпилированные образцы;

– у администраторов, настройщиков, заливщиков: на компьютере – данные о доступе к серверам и веб-интерфейсам управления ботсетями и другой сетевой инфраструктуре;

– у «обнальщиков»: в большом количестве «одноразовые» телефоны, *SIM*-карты, банковские карты, на компьютере – отсканированные изображения паспортов, финансовых и регистрационных документов и т. п.;

– у всех соучастников: средства связи, *SIM*-карты, модемы, специальная техника для усиления приема и передачи сигналов *Wi-Fi*, на компьютерах – клиенты обмена сообщениями, контактные листы, история переписки.

7.4. Допрос

Допрос является одним из самых распространенных следственных действий при расследовании любого преступления. Не являются исключением и преступления в сфере компьютерной информации. Как наиболее важные виды допросов по уголовным делам о хищениях в электронных платежных системах можно выделить: допросы потерпевшего либо представителей пострадавшей организации об обстоятельствах совершенного преступления, предшествующие осмотру места происшествия; допрос свидетелей с целью сбора сведений

для подготовки производства обыска в помещении, используемом подозреваемым в киберкриминальной деятельности и для его задержания; допрос подозреваемого непосредственно после произведенного обыска.

Любому осмотру должны предшествовать определенные подготовительные мероприятия, перечень которых обусловлен конкретными обстоятельствами дела. Например, предварительный допрос лиц, имеющих отношение к преступлению, связанному с хищением денежных средств в системе ДБО. К таким лицам могут быть отнесены генеральный директор предприятия, бухгалтер, системный администратор. Полученные от них сведения помогут не только установить обстоятельства преступления, но также могут быть весьма полезными при производстве судебной компьютерной программно-сетевой экспертизы.

Примерный перечень вопросов, подлежащих выяснению:

1. Каким образом организованы на предприятии компьютерная сеть (при наличии) и доступ к сети Интернет, изменилась ли обстановка с момента хищения?

2. Кто имеет доступ к программе-клиенту ДБО, каково количество выданных токенов?

3. С каких компьютеров осуществляется подключение к программе-клиенту ДБО, какие из них работали в день хищения, с какого из них осуществлялось подключение к клиенту, и кто именно работал за этим компьютером?

4. Каким образом осуществляется подключение к программе-клиенту ДБО (непосредственно со скомпрометированного компьютера, посредством терминала удаленного доступа)?

5. Кто и при каких обстоятельствах узнал о несанкционированном списании средств, какие действия предприняты?

6. Имели ли место отклонения от нормального функционирования компьютеров, подключаемых к клиенту, в период, предшествующий инциденту? В чем именно заключались нарушения в нормальной работе компьютеров?

7. Каков внутренний *IP*-адрес компьютера, скомпрометированного инцидентом (при наличии сети)?

Допрос подозреваемого сразу после проведенного у него обыска тактически целесообразен для выяснения у него сведений об используемых средствах сокрытия криминалистически значимой компьютерной информации. В ходе последующих осмотра и экспертизы изъ-

ятых у него компьютерной техники и устройств мобильной связи, возможно, потребуются пароли либо иные данные для получения доступа к зашифрованным областям, данным и заблокированным устройствам. Важно получить у него эти сведения в тот момент, пока он еще не выработал защитную позицию, направленную на противодействие расследованию.

7.5. Судебная компьютерная экспертиза

Изъятые электронные носители, на которых, по существу, законсервирована компьютерная информация, содержащая вредоносные программы, следы их деятельности, и другие сведения, позволяющие установить обстоятельства преступления, подлежат экспертному исследованию. В процессе исследования перед экспертом необходимо поставить вопросы, разрешение которых позволит прийти к заключению о наличии на представленных к экспертизе объектах компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, а также об их функциональных свойствах. Кроме того, учитывая, что при совершении киберпреступлений используются легальные программы, например для осуществления удаленного управления скомпрометированной системой, необходимо исследовать представленные объекты на предмет наличия ПО либо иной компьютерной информации, которые могли применяться в противоправной деятельности. Если объекты, представленные на исследование, были изъяты у подозреваемого лица, следует проверить их на наличие следов разработки программ, которые могут быть использованы при совершении киберпреступлений, а также программ, предназначенных для анонимизации деятельности пользователя в сети Интернет. В общем, компьютерная программно-сетевая экспертиза позволяет установить многие другие имеющие существенное значение для расследования обстоятельства совершенного преступления либо подготовки к нему.

Вопросы, которые могут быть поставлены на разрешение эксперту по объектам, изъятым с места происшествия:

1. Имеются ли на представленных на исследование объектах программы, предназначенные для несанкционированных пользователем уничтожения, блокирования, модификации, сбора, копирования информации либо для нейтрализации средств защиты компьютерной

информации, или следы деятельности таких программ? Если имеются, каковы их функциональные возможности?

2. Имеются ли на представленных на исследование объектах программы, которые могли быть использованы для несанкционированного удаленного управления компьютером? Если имеются, каковы их функциональные возможности? Имеются ли следы несанкционированного доступа к компьютеру либо попыток осуществления несанкционированного доступа?

3. Имеются ли на представленных на исследование объектах данные, позволяющие определить дату, время, способ, источник загрузки и установки на компьютер программ, перечисленных в вопросах 1–2 настоящего постановления?

4. Имеются ли на представленных на исследование объектах данные о взаимодействии программ, перечисленных в вопросах 1–2 настоящего постановления, с сетевыми ресурсами, используемыми для управления этими программами, а также получения от них и передачи им какой-либо информации? Каковы идентифицирующие признаки этих сетевых ресурсов (*IP*-адреса, имена доменов, полные строки обращений (*URL*)?

5. Имеются ли на представленных на исследование объектах программы, позволяющие без ведома пользователя использовать компьютер для перенаправления сетевого трафика, или следы деятельности таких программ?

6. Имеются ли на представленных на исследование объектах программы, перечисленные в вопросах 1–2, 5 настоящего постановления, установленные с ведома пользователя, либо следы разработки и (или) использования таких программ? Если имеются, каковы их функциональные возможности?

7. Имеются ли на представленных на исследование объектах скрытые и (или) зашифрованные разделы диска и (или) файлы? Каково их содержимое?

8. Имеются ли на представленных к исследованию объектах программы, предназначенные для анонимизации деятельности пользователя в сети Интернет и (или) следы их использования?

Вопросы, которые могут быть поставлены на разрешение эксперту, по объектам, изъятым с места происшествия (альтернативный вариант):

1. Имеется ли на представленных на исследование объектах ПО, способное осуществлять без ведома пользователя уничтожение, бло-

кирование, модификацию, копирование компьютерной информации либо нейтрализацию средств защиты компьютерной информации, следы исполнения которого содержатся на этих объектах? Если такое ПО имеется, то какими функциональными возможностями оно обладает, когда и каким образом оно появилось на объекте, каковы следы его исполнения?

2. Имеется ли на представленных на исследование объектах ПО, используемое для удаленного управления компьютером, а также следы доступа, либо для попыток осуществления доступа к компьютеру с помощью данного ПО? Когда и каким образом оно появилось на объекте, каковы следы его исполнения?

7.6. Типичные ошибки при проведении обыска или осмотра и назначении экспертизы

Наиболее распространенная и, наверное, самая общая ошибка, влекущая многие другие, – это отсутствие либо формальный характер подготовительных мероприятий к проведению следственных действий. Нередко подготовка не учитывает специфики преступной деятельности в сфере компьютерной информации. Например, ошибка в месте производства обыска, когда квартира либо офис были установлены по входящему в помещение интернет-каналу провайдера, в сетевом трафике которого зафиксированы признаки противоправной активности, без проверки версии о скомпрометированном *Wi-Fi*-передатчике, лицом, проживающим или работающим в соседнем помещении. Отсутствие предварительного инструктажа всех участников мероприятия часто приводит к утрате криминалистически значимой информации уже в ходе производства обыска. Следователи и оперативные сотрудники не всегда осознают, насколько легко подозреваемый может уничтожить информацию, закрыв крышку ноутбука либо выдернув силовой кабель.

Участие специалиста в производстве обыска при изъятии электронных носителей информации обязательно. Но в изъятии *USB*-флеш-накопителя особых специальных познаний не требуется. Наоборот, при изъятии компьютерной техники, которая используется для разработки и управления вредоносными программами, для осуществления неправомерного доступа и т. п. специалисту должны предъявляться высокие требования к его профессиональной компетенции.

Поскольку риск утраты компьютерной информации очень высок (гораздо выше, чем риск утраты традиционных доказательств), необходимо в первую очередь допустить к технике специалистов в области компьютерной криминалистики с соблюдением мер предосторожности, например с использованием латексных перчаток, чтобы не были стерты следы рук и потожировые следы.

Излишнее изъятие техники приводит к ничем не обоснованной загрузке экспертов, которые вынуждены подвергать исследованию каждый объект, представленный на экспертизу, даже содержащий информацию, не относящуюся к делу.

Непонимание либо осознанное игнорирование следователем границ профессиональной компетенции эксперта часто приводит к постановке вопросов, которые будут либо проигнорированы в процессе исследования, либо ответы на них будут признаны недопустимыми в ходе проверки в суде. Например, вопрос о «заведомости» в определении вредоносной программы. Эксперт может исследовать лишь функциональные возможности представленной на исследование программы. Вопрос установления умысла находится в исключительной компетенции следствия.

Типичные следственные ошибки:

– отсутствие подготовительных мероприятий;

– привлечение специалиста, не обладающего необходимой компетенцией;

– нарушение очередности криминалистических методов сбора доказательств, влекущее утрату компьютерной информации, имеющей существенное значение для дела;

– формальный подход к организации обыска;

– не обоснованное конкретными обстоятельствами дела изъятие техники;

– направление на экспертизу объектов без их предварительного осмотра с участием специалиста;

– направление на экспертизу всех изъятых по делу объектов без учета мнения специалиста о наличии либо отсутствии на них криминалистически значимой информации;

– постановка перед экспертом вопросов, выходящих за пределы его компетенции;

– возложение на эксперта обязанности по сбору дополнительной информации, имеющей доказательственное значение по делу.

ГЛАВА 8. ОПЕРЕЖАЮЩИЕ ТЕХНОЛОГИИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: KSN – СЕТЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Последние годы повсеместно, и настоящее пособие не исключение, говорят о том, что сегодняшнее научно-техническое, социальное и экономическое развитие общества определяются взрывным ростом информационно-компьютерных технологий. И это действительно так. Цифровизация всех сторон жизни общества привела к тому, что современный человек, реализуя свои потребности посредством использования компьютеров, смартфонов, смарт-часов, спортивных трекеров, «умных» бытовых устройств в огромном объеме сам генерирует информацию, причем делает это непрерывно. Еще одной особенностью настоящего положения дел в цифровой сфере является то, что большая часть этой информации хранится и обрабатывается уже не на пользовательских устройствах, а на ресурсах провайдеров интернет-услуг самого широкого спектра, функционирующих на основе облачных технологий. В 2008 г. редактор научного журнала *Nature* К. Линч ввел в оборот термин «большие данные» (*Big Data*), под которым понимаются любые постоянно обновляющиеся неструктурированные либо частично структурированные данные огромного объема, анализ которых позволяет получить новые знания. Исследователям феномена больших данных изначально было понятно, что для их обработки и анализа требуются новые технические решения и инструментарий. В настоящее время эти задачи решаются разработкой и внедрением технологий машинного обучения (глубокого обучения, искусственных нейронных сетей и т. п.), и запрос на них в обществе огромный.

Но вместе с тем, несмотря на то, что дефиниции современным процессам генерации, обработки и анализа больших данных были даны только в конце 2000-х гг., лидеры рынка информационных технологий задолго до этого, решая прикладные задачи, приступили к разработке и внедрению нового инструментария, дальнейшее развитие которого привело к созданию систем, вплотную приблизившимся к порогу, за которым находится полноценный искусственный интеллект (ИИ). Этапы развития таких систем проиллюстрируем на конкретном примере – технологии *KSN*, принадлежащей АО «Лаборатория Касперского». Под этой аббревиатурой скрывается распределенная облачная инфраструктура *Kaspersky Security Network*, что можно перевести как

Сеть обеспечения безопасности. Данная технология, изначально создававшаяся для сбора информации о результатах работы антивирусных программ, на текущий момент превратилась в огромную систему, способную без участия человека собирать, анализировать, принимать решения и предсказывать работу вредоносного ПО. Чтобы понять, как она работает, необходимо рассмотреть основные вехи истории, в которых произошли события, имеющие отношения к развитию информационных технологий, работе вредоносных программ и эволюции систем обеспечения безопасности в компьютерных сетях.

Весной 2002 г. сотрудники АО «Лаборатория Касперского» столкнулись с проблемой распространения по всему миру нескольких вредоносных программ, таких как *Blaster* и *Sasser*. Несколько лет эти программы, обладающие возможностями самораспространения, беспрепятственно разлетались по сети Интернет, представляя постоянную угрозу для пользователей, независимо от места их географического местонахождения. Помимо необходимости выработки мер по противодействию вредоносным программам этот вопрос был важен для бизнеса, который требовал аналитические данные по уровню востребованности защитных решений в различных странах мира.

Для ответа на поставленный вопрос аналитики сначала использовали методы анализа содержимого вредоносных программ для поиска языковых артефактов, а также выявления упоминаний популярного в разных странах ПО и интернет-ресурсов. Так, каждый образец вредоносного ПО содержал маркер страны распространения. Если, например, в образце были строчки на китайском языке, то он помечался как китайский. Если в строчках упоминались популярные на территории России программы, такие как *The Bat!, Far Manager, ICQ* и т. д., то как российский. Если *America Online* – как американский.

Данный метод маркировки образцов вредоносного ПО был неточным, опирался на субъективное экспертное мнение и не мог ответить на вопрос о распространении программ, содержащих англоязычные или испаноязычные текстовые артефакты. Для устранения таких неточностей в 2005 г. разработчики представили первый прототип технологии, впоследствии получившей название *KSN*.

С самого начала развития информационных технологий одной из главных проблем была передача информации между компьютерами. Вехой этой истории было использование для таких целей дискет. И наряду с распространением вирусных вредоносных программ, с помощью дискет распространялось и антивирусное ПО. С развитием компьютерных

сетей в целом и сети Интернет в частности необходимость в подобных носителях информации отпала. Теперь вредоносные программы могли распространяться и получать команды от злоумышленников через сеть, а антивирусное ПО могло получать обновления баз данных, содержавших информацию о различных вредоносных программах, методах их удаления и восстановления работы компьютера. Будучи запущенным на компьютере, антивирусное ПО записывает в файл определенный журнал о результатах своей работы, и именно этот журнал в качестве обратной связи в 2005 г. начал поступать на серверы, распространяющие обновления для антивирусного ПО «Лаборатории Касперского». Таким образом, в 2005 г. аналитикам впервые удалось построить карту географического распространения обнаруженных вредоносных программ.

На приведенной карте отображен процент уникальных пользователей, атакованных вредоносными программами для мобильных телефонов в стране, по отношению ко всем пользователям мобильного антивируса «Лаборатории Касперского» (*рис. 8.1)*.

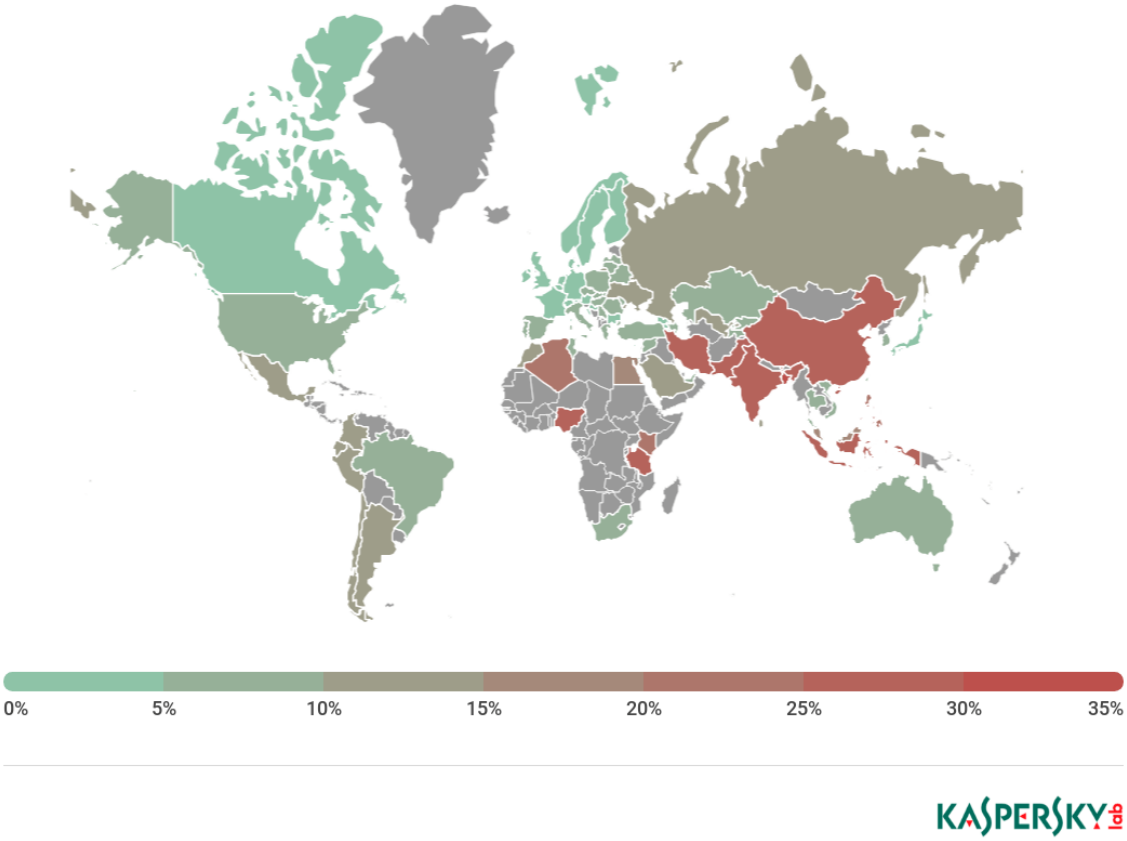


Рис. 8.1. Карта, полученная с использованием *KSN*. III квартал 2018 г., %

Во время работы по анализу данных, собранных таким образом, также выявилась проблема отсутствия способов обнаружения для огромного количества вредоносных программ. Злоумышленники при распространении своих изделий использовали методы постоянного

обновления. То есть точно так же, как антивирусное ПО получает обновление своих баз один раз в час, ресурс в сети Интернет, распространяющий вредоносные программы, получает обновление от автора каждые полчаса. Таким образом, «борьба» вирусов и антивирусов приобрела формат настоящей гонки.

Учитывая, что в 2005 г. антивирусное ПО в основном использовало методы сигнатурного анализа, злоумышленники могли быстро и легко менять сигнатуры своих изделий и использовать методы упаковки исполняемых файлов для обхода систем защиты. Однако при наличии системы обратной связи о результатах работы антивируса аналитики начали разрабатывать целый спектр технологий, направленных на решение задач, поставленных злоумышленниками. Такими технологиями стали:

– эмуляция – технология, позволяющая следить за процессом работы для решения задачи упаковки;

– поиск похожести – технология, позволяющая следить за минимальными изменениями в файлах для поиска обхода сигнатурного анализа;

– «белые» и «черные» списки – технология, позволяющая блокировать любые файлы, не входящие в белый список.

Каждая из этих технологий позволяла бороться с автоматизированными средствами, которые начали использовать злоумышленники для «гонки» с антивирусными компаниями. При этом технология обратной связи 2005 г. использовалась как основное средство для пополнения «белых» и «черных» списков. В 2009 г. «Лабораторией Касперского» была запатентована данная технология. Получение патента также дало и официальное название технологии – *Kaspersky Security Network* (*KSN*).

В течение 2009 г. были получены патенты на несколько способов применения *KSN*: системы и методы для обнаружения неизвестных вредоносных программ; системы и методы обнаружения и предсказания распространения вредоносных программ. Каждый из этих патентов опирается на данные, которые поступают в *KSN* от пользователей программ «Лаборатории Касперского». Примерами применения запатентованных систем и методов могут служить следующие ситуации:

– злоумышленники пытаются замаскировать названия файлов вредоносных программ под системные файлы (например, *SVCH0ST.EXE*, где пятая буква *O* заменена на цифру ноль);

– злоумышленники пытаются обновлять вредоносные программы на ресурсах сети Интернет быстрее выхода обновлений антивирусного ПО (например, сайт *http://virus1.com.ru* содержит файл с именем *virus.exe*, ссылка на который распространяется через электронную почту, и каждый пользователь, посетивший данный сайт, получит уникальную версию вредоносной программы).

В данных примерах пользователь, имея доступ к данным из *KSN* об именах файлов и ссылках на источники файлов, может сделать простой вывод о том, что попытка маскировки под системные файлы и частое изменение файлов на сетевых ресурсах может быть признаком работы и распространения вредоносных программ. Но раз пользователь может сделать вывод на основании таких данных, то можно попытаться научить и компьютер делать то же самое.

Компьютерная система, способная заменить человека в решении какой-либо задачи, называется экспертной. Первая экспертная система, обрабатывающая информацию из *KSN*, была построена на математической модели «Правила подсчета очков». Данные правила предлагали простой способ принятия решения о вредоносности файлов. Суть данного метода основывается на формуле:

$$S = N1 \times K1 + N2 \times K2 + \ldots + NnKn,$$

где S – финальный счет, N – значение верности некоего утверждения (может быть только 1 или 0), K – коэффициент значимости утверждения.

В этом примере при $S = 100$ файл признается вредоносным.

Разберем несколько утверждений, при верности которых мы будем выставлять значение N в формулу для принятия решения:

- Утверждение № 1: Файл загружается с ресурса, используемого злоумышленниками для распространения вредоносных программ.
- Утверждение № 2: Размер файла совпадает с размерами других вредоносных программ, распространяемых этими же злоумышленниками с указанного в утверждении № 1 ресурса.
- Утверждение № 3: Имя файла соответствует имени системного файла, необходимого ОС для работы.
- Утверждение № 4: Файл не имеет цифровой подписи разработчиков ОС.

Предположим 2 ситуации:

1. Злоумышленники распространяют обычную для себя вредоносную программу под видом обновления для ОС. Тогда утвержде-

ния № 1–4 являются истинными, а их значения *N* для решения равны 1.

2. Злоумышленники на самом деле распространяют обновление для ОС со своего ресурса. Тогда утверждения № 1–3 истинны и принимают значение 1, утверждение № 4 ложное и имеет значение 0.

Подсчитаем результат *S* для первой ситуации:

$$S = 1 \times K1 + 1 \times K2 + 1 \times K3 + 1 \times K4.$$

Теперь нам необходимо расставить значения коэффициентов *K* таким образом, чтобы *S* = 100. Для примера определим, что все значения *K* = 25. Таким образом, мы получаем, что:

$$1 \times 25 + 1 \times 25 + 1 \times 25 + 1 \times 25 = 100.$$

Теперь рассмотрим вторую ситуацию, когда злоумышленники подсовывают нам настоящий системный файл. В этом случае формула будет выглядеть как:

$$S = 1 \times K1 + 1 \times K2 + 1 \times K3 + 0 \times K4.$$

После подстановки значений наших коэффициентов *K* получается:

$$1 \times 25 + 1 \times 25 + 1 \times 25 + 0 \times 25 = 75.$$

В первой ситуации *S* = 100, что является достаточным условием для признания файла вредоносным, а во второй ситуации *S* = 75, что недостаточно для признания файла вредоносным.

Теперь, когда наша экспертная система создана, нашей задачей становится создание дополнительных утверждений и подбор коэффициентов значимости для этих утверждений. Эта задача по силам искусственным нейронным сетям, которые могут «обучаться» (подбирать коэффициенты) и давать более точный результат для принятия решений.

После того, как у *KSN* появилась система для принятия решений о вредоносности файлов, актуальной стала задача обратная – научиться определять, не являются ли файлы невредоносными. Обе эти задачи привели к распределению всех возможных файлов на 3 категории:

- файл вредоносный;
- файл «чистый»;
- файл «неизвестный».

Учитывая, что теперь каждый файл возможно отнести к определенной категории, для дальнейшего развития можно начать приме-

нять кластерный анализ, который опять же призван автоматизировать процесс принятия решений, а также способен начать прогнозировать решения в ситуации, когда данных для утверждений нашей экспертной системе не хватает.

Для понимания этой ситуации «раскрасим» каждый файл в соответствии с его категорией (*рис. 8.2*). Например, вредоносные файлы обозначим красным цветом, «чистые» – синим, «неизвестные» – желтым. Учитывая, что каждый из этих файлов обладает огромным количеством данных, которые его характеризуют, мы можем начать строить графы, где к каждому файлу мы будем дорисовывать, например, его размер, имя, ресурс сети, с которого он был загружен, содержимое его языковых артефактов и популярных строк из него (о чем шла речь еще в 2002 г.), результаты работы эмулятора как результат дополнительной технологии, разрабатываемой параллельно с *KSN*, и т. д. Таким образом, каждый из файлов начнет соотноситься с другими файлами (например, у нескольких файлов одинаковое имя или размер), а все файлы будут связываться в группы или кластеры.

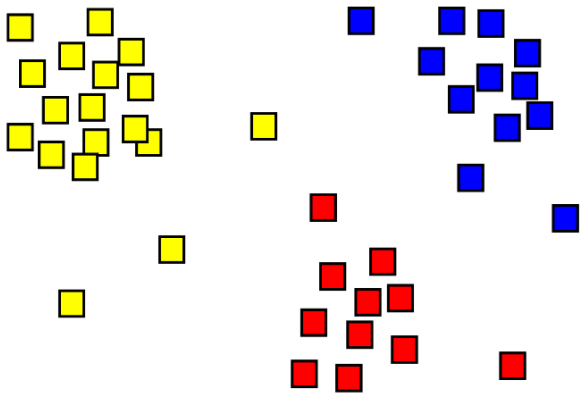


Рис. 8.2. Пример результата кластерного анализа

Данные действия необходимы для следующего результата. Когда появляется новый файл, который мы не можем пока отнести ни к одной из категорий, мы ставим точку на нашем графике и, по мере получения данных об этом файле, начинаем эту точку двигать ближе к одному или другому кластеру. Получается, что даже если у нас нет файла, его содержимого, возможности его проанализировать, не хватает данных о нем, мы можем уже начать предсказывать, в какую категорию он попадет: к красным, синим или желтым.

После того, как появились механизмы принятия решений и предсказаний, важными становятся количество и качество данных, которые попадают в *KSN*. При этом нужно понимать, что система требует огромных вычислительных ресурсов для работы экспертной системы. Хранение данных занимает петабайты, а стоимость оборудования составляет несколько миллионов долларов. В такой ситуации необходима оптимизация процессов обработки файлов и применения алгоритмов свертки и подсчета контрольных сумм. То есть, например, приходится отказываться от загрузки полного содержимого файла, так как его размер может составлять несколько гигабайт, а отправлять в *KSN* только результат обсчета его хеш-суммы. Но за этим, казалось бы, ограничением кроется один важный факт, оборачивающийся в выгоду.

Хеш-суммы бывают разными, и в основном их используют в криптографии. При этом, например, для хранения паролей используются результаты работы хеш-функций, чтобы два очень похожих друг на друга пароля (различающихся, например, одним символом) были очень несхожи.

```
$ echo password | md5sum
286755fad04869ca523320acce0dc6a4  –

$ echo password1 | md5sum
10b222970537b97919db36ec757370d2  –
```

Пример подсчета хеш-сумм для паролей *password* и *password1* в ОС *Linux*

Однако возможна и обратная ситуация, когда очень непохожие пароли будут преобразовываться в одинаковые хеш-суммы. Получается, что когда злоумышленники пытаются сбить сигнатурный анализ антивирусного ПО, над сигнатурой можно провести операцию свертки, чтобы она не была «чувствительна» к действиям злоумышленников. Таким образом, отсутствие файлов, недостаток данных в *KSN*, высокую стоимость оборудования можно обернуть в выгоду.

```
MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQA
YT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9E
qJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEE
FLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaN
Npgq+CXsPwfITDbDDmdrRIiUEUw6o3pt5pNOskfOJbMan2TZu
```

Пример сигнатуры для обнаружения вредоносной программ *Petya*

Выгода заключается также и в том, что сигнатура, которая является частью программы, написанной злоумышленником, отражает алгоритм, действия, способ мышления автора. Получается, что программы можно начать распределять не только на «чистые» и вредоносные, но и по их авторству.

На текущий момент *KSN* является одной из самых развитых технологий для определения вредоносных программ, которая может не только принимать решения, но и обучаться, предсказывать, определять авторство. Система, которая задумывалась как средство для ответа на вопрос о географическом распределении вредоносных программ, вплотную приблизилась и термину «искусственный интеллект». И пока многие спорят о достижимости (или недостижимости) уровня развития компьютерных систем до человеческого интеллекта, *KSN* уже можно сравнить с музыкальным критиком из анекдота, который сказал: «Вы мне хоть ногами по роялю постучите, я вам все равно скажу музыкальный стиль, год и автора».

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования рассмотрены вопросы уголовно-правовой характеристики преступлений, совершенных с помощью компьютерных технологий с точки зрения Европейской конвенции о киберпреступности и иных международно-правовых актов противодействия киберпреступности, а также проведен анализ изменений, внесенных в главу 28 УК РФ.

Подробным образом разобрана характеристика компьютерных преступлений. Выделены орудия и средства совершения компьютерных преступлений. Классифицировано вредоносное ПО, выступающее в том числе и средством совершения компьютерного преступления. Отдельным разделом рассмотрены программно-аппаратные технологии совершения компьютерных преступлений.

Проработаны аспекты хищения в электронных платежных системах, включая способы совершения подобных преступлений в электронных платежных системах. Рассмотрены функциональные возможности современного вредоносного ПО, используемого для совершения преступлений в платежных системах. Приведена попытка выявить причины и условия, побуждающие совершать преступления.

Показана взаимосвязь компьютерных преступлений как одного из проявлений кибертерроризма.

Немало внимания уделено особенностям сбора цифровых следов и превращения их доказательства по делам о компьютерных преступлениях, в том числе вопросам подготовки и производства следственных действий на всех этапах.

Приведены типичные ошибки при проведении следственных действий и назначении экспертизы.

Учебное пособие

Чекунов Игорь Геннадьевич,
кандидат юридических наук

Рядовский Игорь Анатольевич,

Пузарин Андрей Валерьевич,

Сабитов Руслан Рамилевич,

Голованов Сергей Юрьевич

Русскевич Евгений Александрович,
кандидат юридических наук

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Редактор *Фомин И. Е.*
Компьютерная верстка *Фомин И. Е.*

Московский университет МВД России имени В.Я. Кикотя
117437, г. Москва, ул. Академика Волгина, д. 12

Подписано в печать 14.10.2019 г.	Формат 60×84 1/16	Тираж	70 экз.
Заказ № 1950	Цена договорная	Объем	8,32 уч.-изд. л. 10,23 усл. печ. л.