Е. Р. Россинская*,
И. А. Рядовский**

СОВРЕМЕННЫЕ СПОСОБЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ И ЗАКОНОМЕРНОСТИ ИХ РЕАЛИЗАЦИИ[1]

Аннотация. *В статье отмечается, что интеграция современных информационных технологий во все сферы человеческой деятельности привела к информатизации и компьютеризации преступности, когда с использованием компьютерных средств и систем возможно совершение практически любых преступлений. Отмечается общность ряда элементов механизма компьютерных преступлений, включающая сведения о способах этих преступлений.*

Способы компьютерных преступлений рассмотрены с позиций новой частной теории информационно-компьютерного обеспечения криминалистической деятельности, предметом которой служат закономерности возникновения, движения, собирания и исследования компьютерной информации при расследовании преступлений. Объектами являются компьютерные средства и системы, особенности криминалистических технологий собирания (выявления, фиксации, изъятия) и исследования этих объектов для получения доказательственной и ориентирующей информации. С современных позиций способ преступления — это детерминированная личностью, предметом и обстоятельствами преступного посягательства система действий субъекта, направленная на достижение преступной цели и объединенная единым преступным замыслом. Способы преступления делятся на полноструктурные, включающие подготовку, совершение и сокрытие, и неполноструктурные, когда один или два элемента отсутствуют. На формирование способа преступления оказывают влияние объективные и субъективные факторы, что определяет детерминированность и повторяемость способов преступления.

Рассматриваются основные способы компьютерных преступлений: направленные на сокрытие несанкционированного доступа к компьютерным средствам и системам; использование троянских программ различного назначения; заражение компьютерных систем вирусами; использование аппаратно-программных комплексов для массовых кампаний распространения вредоносного программного обеспечения на мобильные устройства; компьютерных атак на локальные корпоративные сети и др.

* *Россинская Елена Рафаиловна,* доктор юридических наук, профессор, директор Института судебных экспертиз, заведующий кафедрой судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), заслуженный деятель науки Российской Федерации, почетный работник высшего профессионального образования Российской Федерации
elena.rossinskaya@gmail.com
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** *Рядовский Игорь Анатольевич,* руководитель отдела расследования компьютерных инцидентов АО «Лаборатория Касперского», почетный работник прокуратуры Российской Федерации
igor.ryadovsky@kaspersky.com
125212, Россия, г. Москва, Ленинградское ш., д. 39а, стр. 3

Установлено, что криминалистической закономерностью формирования и реализации компьютерных преступлений является обязательный этап приготовления к преступлению, включающий в то же время действия по сокрытию следов преступления, т.е. способы компьютерных преступлений являются полноструктурными.

Ключевые слова: *информационно-компьютерное обеспечение; компьютерное преступление; механизм преступления; способ преступления; полноструктурный способ, неполноструктурный способ; вредоносная программа; несанкционированный доступ; технологии Bootkit; технологии Rootkit; «бестелесная» технология; технологии криптования, технология обфускации; троянская программа; программа-червь; программа-вирус; бот-ферма; атака на локальные сети.*

DOI: 10.17803/1729-5920.2019.148.3.087-099

ВВЕДЕНИЕ

Лавинообразно возрастающий процесс цифровизации, проникновение современных компьютерных технологий практически во все сферы человеческой деятельности — экономическую, социальную, управленческую, культурную и другие — существенно повлиял на жизнь социума, в том числе не мог не затронуть и судопроизводство, оказав огромное влияние на видоизменение преступной деятельности в целом. Наряду с возникновением новых видов преступлений в сфере компьютерной информации, практически любые преступления: присвоения, кражи, мошенничества, фальшивомонетничество, лжепредпринимательство, преступления в банковской сфере и многие другие — совершаются в настоящее время с помощью компьютерных средств и систем. Развитие цифровых технологий постоянно порождает все новые виды преступлений и способы их совершения и сокрытия. В связи с массовым распространением средств мобильной коммуникации возникли новые виды преступлений, такие как создание и распространение вредоносных программ для мобильных телефонов, использование мобильных средств связи для совершения мошенничеств, вымогательств, поджогов, взрывов, террористических актов и пр.

Все эти преступления нами ранее было предложено именовать «компьютерными преступлениями», причем мы неоднократно подчеркивали, что дефиниция «компьютерное преступление» должна употребляться не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку она связана не с квалификацией, а именно со способом преступления и, соответственно, с методикой его раскрытия и расследования. Компьютерные преступления имеют общую родовую криминалистическую характеристику, включающую сведения о способах преступлений, лицах, совершивших их, сведения о потерпевшей стороне и об обстоятельствах, способствующих и препятствующих данным преступлениям[2].

Теме расследования компьютерных преступлений, в первую очередь преступлений в сфере компьютерной информации, посвящен целый ряд литературных источников, однако эти работы носят неупорядоченный, фрагментарный характер. Полагаем, это связано с тем, что, к сожалению, в криминалистической науке пока мало изучены компьютерные средства и системы — носители криминалистически значимой компьютерной информации, сама информация в цифровом виде, являющиеся объектами криминалистического исследования; закономерности возникновения, движения и видоизменения потоков криминалистически значимой информации с использованием компьютерных средств и систем. Исключение составляет фрагментарное рассмотрение этих вопросов в методике расследования преступлений в сфере компьютерной информации.

Большинству криминалистов-практиков возможности получения криминалистически значимой компьютерной информации, имеющей доказательственное значение, практически неизвестны, что обусловлено неразработанностью теоретических и технологических аспектов

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003/18.

информационно-компьютерного обеспечения криминалистической деятельности.

Компьютерная информация применительно к процессу доказывания может быть определена как фактические данные, обработанные компьютерной системой и (или) передающиеся по телекоммуникационным каналам, а также доступные для восприятия, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного, гражданского или административного дела[3].

Для решения вышеуказанных проблем нами начата разработка новой частной криминалистической теории: теории информационно-компьютерного обеспечения криминалистической деятельности, предметом которой, по нашему мнению, могут служить закономерности возникновения, движения, собирания и исследования компьютерной информации при расследовании преступлений. Объектами являются компьютерные средства и системы, особенности криминалистических технологий собирания (выявления, фиксации, изъятия) и исследования этих объектов для получения доказательственной и ориентирующей информации[4].

Поскольку криминалистические методы и средства все шире востребуются гражданским и административным судопроизводством, где также в процесс доказывания широко интегрированы компьютерные средства и системы в целях получения участниками процесса доказательственной и ориентирующей информации, необходимо включить в предмет данной теории и закономерности, связанные с рассмотрением дел в гражданском. арбитражном, административном процессе, производством по делам об административных правонарушениях. Однако приоритет, по нашему мнению, должен быть отдан раскрытию и расследованию преступлений, поскольку общей и главной задачей криминалистической науки является борьба с преступностью[5].

Для исследования закономерностей возникновения и движения криминалистически значимой компьютерной информации обратимся к криминалистической дефиниции механизма преступления, который представляет собой сложную динамическую систему, определяющую содержание преступной деятельности. Элементами механизма преступления являются: субъекты преступления; отношение субъекта преступления к своим действиям, их последствиям, соучастникам; предмет посягательства; способ преступления; преступный результат; обстановка преступления (место, время и другие относящиеся к ней обстоятельства); поведение и действия лиц, оказавшихся случайными участниками события, и др.[6]

Одним из важнейших элементов механизма преступления является способ преступления.

Способ преступления, по классическому определению Г. Г. Зуйкова, «представляет собой систему объединенных единым замыслом действий преступника (преступников) по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами, действий, сопряженных с использованием соответствующих орудий и средств»[7]. Другими словами, способ преступления — это детерминированная личностью, предметом и обстоятельствами

---

2 *Россинская Е. Р.* Криминалистика : учебник для вузов. М. : Норма: Инфра-М, 2016. С. 440—442 ; *Аверьянова Т. В.*, *Белкин Р. С.*, *Корухов Ю. Г.*, *Россинская Е. Р.* Криминалистика : учебник для вузов. Изд. 4-е, перераб. и доп. М. : Норма: Инфра-М, 2014. С. 903—905.

3 *Аверьянова Т. В., Белкин Р. С.*, *Корухов Ю. Г.*, *Россинская Е. Р.* Указ. соч. С. 904.

4 *Россинская Е. Р.* Концепция частной криминалистической теории «информационно-компьютерное обеспечение криминалистической деятельности» // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIII Международной науч.-практ. конференции : в 2 т. Иркутск : Восточно-Сибирский институт МВД РФ, 2018. С. 114.

5 *Россинская Е. Р.* Криминалистика. С. 20 ; Криминалистика : учебник для вузов / под общ. ред. А. Г. Филиппова. 4-е изд., перераб. и доп. М. : Высшее образование, 2017. С. 20.

6 *Россинская Е. Р.* Криминалистика. С. 17 ; Криминалистика : учебник студентов для вузов / под ред. А. Ф. Волынского, В. П. Лаврова. 2-е изд., перераб. и доп. М. : Юнити-Дана: Закон и право, 2008. С. 27.

7 *Зуйков Г. Г.* Криминалистическое учение о способе совершения преступления : автореф. дис. … д-ра юрид. наук. М. : Высш. школа МВД СССР, 1970. С. 10 ; *Он же.* Основы криминалистического учения о способе совершения и сокрытия преступления. Гл. 3 // Криминалистика : учебник для юридических вузов МВД СССР / под ред. Р. С. Белкина, В. П. Лаврова, И. М. Лузгина. М. : Академия МВД СССР, 1987. Т. 1. С. 52.

преступного посягательства система действий субъекта, направленная на достижение преступной цели и объединенная единым преступным замыслом. В этой системе могут быть выделены действия по подготовке, совершению и сокрытию следов преступления[8]. В зависимости от этого способы преступления делят на полноструктурные и неполноструктурные. Полноструктурный способ включает действия, относящиеся ко всем его элементам: подготовке, совершению и сокрытию. В тех случаях, когда преступление совершается без предварительной подготовки или когда субъект преступления не планирует действий по его сокрытию, налицо неполноструктурный способ совершения преступления. При этом возможно формирование самостоятельного способа сокрытия преступления[9].

Как отмечал Р. С. Белкин, способ совершения преступления, понимаемый как система действий преступника по подготовке, совершению и сокрытию преступления, будучи в целом отражаемым объектом, как элемент объективной стороны преступления в то же время своими составляющими (действия, средства действий) служит средством отражения в среде события преступления[10]. Кроме того, «следы определенного способа совершения преступления указывают не только на совершенные действия, но и на обстоятельства, детерминировавшие способ совершения преступления, определившие состав и характер совершенных действий, в частности по характеру совершенных действий представляется возможным предположительно судить об определивших способ совершения преступления качествах личности»[11].

На формирование способа преступления оказывают влияние объективные и субъективные факторы, что определяет детерминированность и повторяемость способов преступления. Г. Г. Зуйков отмечает, что «абсолютная повторяемость способов преступлений во всех их признаках полностью исключена. Способы преступлений повторяются, если сохраняется действие определенных факторов, их детерминирующих (мотив и цель преступления, объективная обстановка его совершения, качества личности преступника, особенности предмета преступного посягательства и т.д.), а так как детерминирующие факторы изменяются и в количественном, и в качественном отношениях, то неизбежно изменяются и способы совершения преступлений, сохраняя, однако, некоторую совокупность повторяющихся признаков»[12].

Как отмечает В. Н. Чулахов, среди факторов, определяющих способ преступления, значительную роль играют психофизиологические свойства личности преступника, в частности навыки и привычки. В способе преступления отражаются два вида навыков — общего значения, возникшие вне связи с совершением преступления, и преступные, сформированные в процессе противоправной деятельности. Навыки преступного характера формируются в ходе подготовки к преступлению и совершенствуются при повторных аналогичных преступлениях[13]. Превращение некоторых самостоятельных элементов способа в навык и переход их на уровень автоматизированных, подсознательных актов является одной из закономерностей формирования способа неоднократно совершаемых однородных преступлений, т.е. формируется «преступный почерк».

СПОСОБЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Описание способов компьютерных преступлений начнем с действий по сокрытию преступниками своих данных при использовании сети Интернет с целью предотвращения идентификации их личности. Для сокрытия своего адреса преступники используют различные анонимные компьютерные сети и сервисы, специально созданные для этих целей.

Одним из таких способов является использование VPN-сервисов (англ. Virtual Private

---

8 *Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р.* Указ. соч. С. 62.

9 *Зуйков Г. Г.* Основы криминалистического учения о способе совершения и сокрытия преступления. С. 50—51.

10 *Белкин Р. Р.* Курс криминалистики. 3-е изд., доп. М. : Юнити-Дана, Закон и Право, 2001. С. 71.

11 *Зуйков Г. Г.* Криминалистическое учение о способе совершения преступления. Гл. 6 // Криминалистика / под ред. Р. С. Белкина, И. М. Лузгина. М. : Академия МВД СССР, 1978. Т. 1. С. 60.

12 *Зуйков Г. Г.* «Модус операнди», кибернетика, поиск // Кибернетика и право. 1970. С. 50.

13 *Чулахов В. Н.* Криминалистическое учение о навыках и привычках человека : монография / под ред. Е. Р. Россинской. М. : Юрлитинформ, 2007. С. 206—207.

Network — виртуальная частная сеть)[14]. Технологии VPN обеспечивают шифрование сетевого трафика между компьютером пользователя и VPN-прокси-сервером, который является шлюзом выхода в сеть Интернет и, соответственно, скрывает реальный IP-адрес пользователя. Если требуется высокий уровень конспирации, преступники арендуют у провайдеров хостинговых услуг вычислительные мощности практически в любой точке мира, на которых настраивают собственные VPN-серверы либо виртуальные машины, с которых, используя сторонние VPN-сервисы, выходят в сеть Интернет.

Другой способ, использование которого позволяет скрыть свой IP-адрес, — The Onion Routing, TOR (луковая маршрутизация второго поколения), это технология и программное обеспечение для обмена данными с многослойным шифрованием с помощью системы прокси-серверов, обеспечивающих анонимное сетевое подключение[15].

Троянская программа, обладающая функциональными возможностями VPN-прокси-сервера, также позволяет преступникам создать бот-сеть из компьютеров, зараженных такой программой, и использовать ее для сокрытия своего IP-адреса.

Помимо упомянутых способов анонимизации своих действий в сети Интернет путем построения цепочки прокси-серверов, преступники для этих целей применяют и другие криминальные либо полукриминальные схемы, например через несанкционированное подключение к сторонним беспроводным точкам доступа (Wi-Fi-роутерам) или с помощью беспроводных модемов мобильной связи с сим-картами, оформленными на посторонних 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, правовой режим которой во многих странах мира, в том числе в России, остается неопределенным.

Разработка планов преступной деятельности, координация мероприятий на стадии подготовки к совершению преступления, согласование совместных действий осуществляются соучастниками с применением сетевых протоколов обмена сообщениями, обеспечивающих безопасность передачи данных. Одной из наиболее востребованных реализаций коммуникации в криминальной среде является XMPP-протокол (eXtensible Messaging and Presence Protocol) обмена мгновенными сообщениями, известный еще как Jabber-протокол (буквально — болтовня), который предоставляет возможность настроить свой собственный Jabber-сервер, обеспечивающий шифрование канала[16].

К мерам по сокрытию следов преступления можно отнести также способы, с помощью которых преступники оказывают противодействие осмотру и изъятию компьютерной информации, содержащейся в их компьютерных средствах и системах, имеющей криминалистическое значение. Эти цели достигаются шифрованием компьютерных данных с помощью специализированного программного обеспечения либо возможностью быстрого уничтожения таких данных с использованием специальных программ или устройств.

Для сокрытия следов несанкционированного доступа и вредоносной активности на компьютере пользователя применяются различные меры технического характера, как прошедшие проверку временем технологии шифрования (криптования) и обфускации (obfuscate — делать неочевидным, запутанным), так и новые приемы и методы — «бестелесная» технология, технологии Bootkit, Rootkit 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 программным обеспечением и их исследование специалистами по информационной безопасности.

Вредоносные программы, функционирующие только в оперативной памяти компьютера

---

[14] *Куроуз Д., Росс К.* Компьютерные сети: нисходящий подход. 6-е изд. М., 2016. С. 794—795.

[15] *Ligh M., Adair S., Hartstein B., Richard M.* Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Indianapolis, 2010. Pp. 2—5.

[16] *Торичко Р. С., Клишина Н. Е.* Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. 2018. № 3. С. 181.

и не сохраняющиеся на энергонезависимых запоминающих устройствах, именуют «бестелесными». При отключении питания компьютера, например при его перезагрузке, программа стирается. Такие программы используются преступниками для сокрытия своей активности от антивирусного программного обеспечения[17].

Технология Bootkit применяется для сокрытия вредоносного кода от антивирусного программного обеспечения и для получения максимальных привилегий в системе. Для реализации этого способа вредоносной программой модифицируется, например, главная загрузочная запись (англ. master boot record, MBR), которая считывается процессором еще до начала загрузки операционной системы, а вредоносный код в зашифрованном виде записывается в не используемую операционной системой область дискового пространства. При включении компьютера загрузчик еще до старта операционной системы расшифровывает и загружает в оперативную память вредоносный код[18].

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

Как видно из перечисленных мер, предпринимаемых преступниками с целью сокрытия следов несанкционированного доступа к компьютерным системам и информации пользователя, весьма значительное количество таких деяний совершается с помощью вредоносного программного обеспечения. Преступники используют вредоносные программы для значительного усиления своих возможностей, то есть в криминалистическом плане вредоносная программа является орудием совершения преступления[19].

В уголовно-правовом смысле определение вредоносной программы изложено в ст. 273 УК РФ, согласно которой под вредоносной программой понимается компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. К таким программам следует отнести не только специально разработанное, но и модифицированное легальное программное обеспечение, дополнительные функциональные возможности которого вследствие модификации наделяют его признаками вредоносности.

Заметим, что в качестве орудия совершения преступления может быть использована и легальная программа, функциональность которой предоставляет преступникам возможность достижения своих целей. Большинство легальных программ, используемых преступниками в противоправной деятельности, предназначены для удаленного несанкционированного доступа к компьютеру, управления системой и ее администрирования, например: RMS, Ammyy Admin, TeamViewer и LiteManager. Эти программы обладают функциональными возможностями, достаточными для достижения преступных целей, и определяются антивирусным программным обеспечением с менее критичным именем как условно опасные, в связи с чем пользователи не видят в них особой угрозы. Кроме того, многие из этих программ являются доверенными программами пользователя, установлены с его ведома и не вызывают у него подозрений.

В определенных случаях, например, когда необходимо отключить оповещение пользователя о работе программы либо ее модулей, такие программы подвергаются незначительной модификации, которая может привести к изменению их поведения (набора действий) в системе, которое будет соответствовать другому классу определяемых антивирусным программным обеспечением объектов — Malware (категории вредоносных программ).

Один из таких способов реализуется с помощью технологии DLL Hijacking[20], эксплуатирующей особенности функционирования операционной системы (ОС) Windows. Способ заключается в помещении в одну папку с фай-

---

[17] *Zeltser L.* The History of Fileless Malware — Looking Beyond the Buzzword // URL: https://zeltser.com/fileless-malware-beyond-buzzword (дата обращения: 05.01.2019).

[18] *Matrosov A., Rodionov E.*, *Bratus S.* Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. No Starch Press, 2015. P. 304.

[19] *Чекунов И. Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9—22.

[20] The MITRE Corporation. CWE-427: Uncontrolled Search Path Element // URL: https://cwe.mitre.org/data/definitions/427.html (дата обращения: 05.01.2019).

лом программы удаленного управления вредоносного библиотечного файла (dll-библиотеки), причем с таким же именем, что и расположенная в другой директории легальная библиотека. При запуске программа 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.

Самая общая классификация, широко применяемая в настоящее время для систематизации видов вредоносных программ, выделяет из класса вредоносных программ (Malware) следующие подклассы: программы-вирусы (Virus), программы-черви (Worm) и троянские программы (Trojan)[21].

К вирусам относятся программы, которые обладают способностью к саморазмножению и распространению по локальным ресурсам компьютера. Программы-черви способны к саморазмножению и распространению по компьютерным сетям. Таким образом, два подкласса вредоносных программ — вирусы и черви — без ведома пользователя саморазмножаются на компьютерах и в компьютерных сетях, при этом каждая последующая копия также обладает способностью к саморазмножению.

Проиллюстрируем это на примере. В мае 2017 г. была осуществлена одна из наиболее масштабных за обозримое время атака с применением программы-шифровальщика WannaCry. Только за один день эта вредоносная программа атаковала компьютеры пользователей более чем в 74 странах. 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[22].

Программы, относящиеся к третьему подклассу, — троянские программы — не умеют создавать свои копии и неспособны к самовоспроизведению. В этом случае распространение копий по сети и заражение удаленных компьютеров происходит по команде с сервера управления.

Основным признаком, который служит для дифференцирования троянских программ, является вид действия (поведение), которое они выполняют на компьютере, например:

— программы-шпионы (Trojan-Spy) предназначаются для ведения электронного шпионажа за пользователем, в том числе для перехвата вводимых с клавиатуры данных, изображений экрана, списка активных приложений;
— программы-банкеры (Trojan-Banker) создаются с целью поиска и копирования пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам;
— программы-шифровальщики (Trojan-Ransom) модифицируют пользовательские данные на компьютере либо блокируют работу компьютера с целью получения выкупа за восстановление доступа к информации;
— программы для удаленного управления (Trojan-Backdoor) обеспечивают скрытое удаленное управление компьютером и полный доступ к пользовательской информации;
— программы-загрузчики (Trojan-Downloader, Trojan-Dropper) осуществляют загрузку и установку на компьютер вредоносных программ и их новых версий;
— программы для эксплуатации программных уязвимостей (Exploit) эксплуатируют уязвимости программного обеспечения пользователя.

---

[21] Энциклопедия Лаборатории Касперского. Классификация детектируемых объектов. Вредоносные программы // URL: https://encyclopedia.kaspersky.ru/knowledge/malicious-programs (дата обращения: 05.01.2019).

[22] *Чекунов И. Г., Рядовский И. А., Иванов М. А.* [и др.] Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учеб. пособие / под ред. И. Г. Чекунова. М. : Московский университет МВД России имени В. Я. Кикотя, 2018. С. 28—29.

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 программным обеспечением 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: поиск файлов по именам, запись истории нажатий клавиш клавиатуры, запись видео и создание снимков экрана, копирование буфера обмена, блокирование и нарушение работы операционной системы, получение от сервера управления команд на запуск дополнительных программных модулей, отправка собранной информации на сервер управления и т.п.

Для загрузки троянских программ в компьютерную систему без ведома пользователя применяют различные способы:

— рассылка электронных писем, содержащих вредоносное вложение;
— применение связок эксплойтов при веб-серфинге пользователей в сети Интернет;
— внедрение вредоносного кода в распространяемое легальное программное обеспечение;
— 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 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 внешний интернет-ресурс, при переходе по которой компьютер пользователя подвергается атаке набором эксплойтов. При успешном срабатывании одного из эксплойтов на компьютер пользователя загружается вредоносное программное обеспечение. При необходимости, когда возможности совершения несанкционированных действий на компьютере пользователя ограничены правами его учетной записи, преступниками может быть применен локальный эксплойт для повышения привилегий.

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.

Описанные способы 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 программное обеспечение свой вредоносный код.

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 программного обеспечения 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.

Помимо программных средств, в более редких случаях способами компьютерных преступлений служат специально созданные в преступных целях электронно-вычислительные устройства и программы к ним. Подобные комплексы могут быть как достаточно простыми (например, устройство, скрыто устанавливающееся в разрыв интерфейса клавиатуры для перехвата нажатия клавиш), так и более сложными (например, компьютерное устройство размером с USB-флеш-накопитель с собственным сетевым адаптером и установленной специальной программой удаленного управления предоставляет преступнику возможность получить несанкционированный доступ

к удаленной компьютерной системе; для этого устройство скрыто подключается к целевой системе, например корпоративной компьютерной сети, в месте, исключающем его визуальное обнаружение, для чего нередко в преступление вовлекают работника пострадавшей организации).

К более сложным техническим решениям, создаваемым для совершения преступлений, применимо иное название — аппаратно-программные комплексы. К ним 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 программного обеспечения на мобильные устройства под управлением ОС Android посредством СМС-рассылки либо для DDoS-атак.

Весьма существенную угрозу для банковской сферы представляют аппаратно-программные комплексы, разработанные для хищения денежных средств из банкоматов, — так называемые Black Box. Такой комплекс является, по сути, мини-компьютером со специальным программным обеспечением, который подключают к диспенсеру (механизму выдачи денег) вместо штатного компьютера, расположенного в сервисной зоне банкомата. После этого управление банкоматом может осуществляться с помощью технологий беспроводной передачи данных, например со смартфона.

Глобальная сеть Интернет является всемирной системой объединенных компьютерных сетей, поэтому представляется необходимым уделить внимание таким способам осуществления несанкционированного доступа, как компьютерные атаки на локальные сети.

Согласно Национальному стандарту ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»[23] «под компьютерной атакой понимается целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств» (п. 3.11). Фактически под признаки компьютерной атаки подпадают все способы осуществления несанкционированного доступа к компьютерным системам, упомянутые в настоящей статье. Однако именно атаки на локальные сети позволяют наиболее полно рассмотреть приемы и методы, используемые преступниками с этой целью.

Виды компьютерных атак на локальные корпоративные сети могут быть разными:

— внешняя атака на сетевую инфраструктуру организации либо на компьютерные системы, которым разрешено удаленное подключение к локальной сети;
— 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 программного обеспечения, установленного на компьютерах организации, либо ошибках в настройках сетевого оборудования.

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.

На этой основе способы компьютерных преступлений в зависимости от доступа к компью-

[23] ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27.12.2006 № 374-ст).

терным средствам и системам можно подразделить:

— на способы, связанные с удаленным доступом к компьютерным средствам и системам посредством использования компьютерной коммуникационной сети (локальной или глобальной — Интернет);

— способы, связанные с непосредственным доступом к компьютерным средствам и системам.

В других случаях вовлечение потерпевшего, в той или иной степени, является необходимым условием доведения преступных намерений до конца. Непосредственная эксплуатация уязвимостей человеческого фактора предусматривает прямое общение с потерпевшим с применением навыков социальной инженерии, то есть системы психологических приемов и методов, склоняющих потерпевших к совершению определенных действий в интересах преступников, например к разглашению уникального кода, присланного в СМС-сообщении для авторизации на сетевом ресурсе, либо к самостоятельной загрузке программы удаленного администрирования на свой компьютер и предоставлению реквизитов доступа к нему мошеннику.

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 программного обеспечения и оборудования предоставляет широкий спектр возможностей для получения несанкционированного доступа к конфиденциальной информации. Так, один из широко известных и применяемых способов получения несанкционированного доступа к компьютерной сети — это проведение атаки с применением различных методов сканирования портов сетевых узлов, то есть виртуальных точек входа-выхода сетевого трафика, обслуживающих определенные локальные сервисы. Обнаружив в результате сканирования открытый порт, который обычно используется одной из распространенных программ удаленного администрирования, преступники могут получить доступ к системе перебором реквизитов доступа (пары логин — пароль).

Для доступа к корпоративным компьютерным системам преступники могут воспользоваться и уязвимостью 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. В связи с этим можно разграничить способы получения несанкционированного доступа к компьютерным системам и сетям по степени вовлеченности протерпевшего в этот процесс:

— эксплуатация уязвимостей аппаратного и программного обеспечения;
— использование недостатков организационного и технического характера корпоративных охранных систем;
— применение методов социальной инженерии.

ЗАКЛЮЧЕНИЕ

Подводя итоги, хотелось бы отметить, что вследствие продолжающегося бурного развития информационно-коммуникационных технологий, в том числе средств криптографии, такая же динамика присутствует и в освоении преступниками способов компьютерных преступлений, сопряженных с несанкционированным доступом к компьютерным средствам и системам. При этом отходят на второй план и используются только в качестве вспомогательных распространенные еще в недавнем прошлом способы преступлений, такие как, например, перехват сетевого трафика, потерявший свою эффективность с точки зрения преступников в результате массового перехода сетевых сервисов с HTTP-протокола, предусматривающего открытую передачу данных, на протокол HTTPS, обеспечивающий шифрование сетевого трафика между конечными устройствами[24].

Полагаем, что представленный в данной статье анализ способов компьютерных преступлений наглядно показывает, что способы компьютерных преступлений являются полноструктурными. Основной криминалистической закономерностью формирования и реализации способа преступления с использованием информационных компьютерных технологий является то обстоятельство, что подготовка обычно предусматривает действия по сокрытию, т.е.

[24] *Helme S.* Alexa Top 1 Million Analysis — February 2018 // URL: https://scotthelme.co.uk/alexa-top-1-million-analysis-february-2018 (дата обращения: 05.01.2019).

при совершении компьютерных преступлений, сопряженных с несанкционированным доступом, характерно осуществление преступниками комплекса мер, предшествующих покушению на преступление, которые направлены и на сокрытие его следов.

Применительно к способам компьютерных преступлений можно обозначить следующие закономерности частной теории информационно-компьютерного обеспечения криминалистической деятельности:

— закономерности формирования и реализации способа преступления, совершаемого с использованием информационных компьютерных технологий (связь способа с личностью преступника, зависимость способа от конкретных обстоятельств совершения преступления и т.д.);
— закономерности отражения в компьютерных средствах и системах информации о связях действий и их результатов, повторяемости действий в похожих ситуациях, стереотипах действий субъектов при совершении преступлений;
— закономерности возникновения и развития обстоятельств, связанных с преступлением, сопряженным с использованием компьютерных средств и систем (как до, так и после его совершения), и значимых для расследования.

БИБЛИОГРАФИЯ

1. *Аверьянова Т. В.*, *Белкин Р. С.*, *Корухов Ю. Г.*, *Россинская Е. Р.* Криминалистика : учебник для вузов. — Изд. 4-е, перераб. и доп. — М. : Норма: Инфра-М, 2014. — 928 с.
2. *Белкин Р. Р.* Курс криминалистики. — 3 изд., доп. — М. : Юнити-Дана, Закон и право, 2001. — 837 с.
3. *Зуйков Г. Г.* «Модус операнди», кибернетика, поиск // Кибернетика и право. — 1970. — С. 46—56.
4. *Зуйков Г. Г.* Криминалистическое учение о способе совершения преступления : автореф. дис. … д-ра юрид. наук. — М. : Высш. школа МВД СССР, 1970. — 31 с.
5. *Зуйков Г. Г.* Криминалистическое учение о способе совершения преступления. Гл. 6 // Криминалистика / под ред. Р. С. Белкина, И. М. Лузгина. — М. : Академия МВД СССР, 1978. — Т. 1. — 384 с.
6. *Зуйков Г. Г.* Основы криминалистического учения о способе совершения и сокрытия преступления. Гл. 3 // Криминалистика : учебник для юридических вузов МВД СССР / под ред. Р. С. Белкина, В. П. Лаврова, И. М. Лузгина. — М. : Академия МВД СССР, 1987. — Т. 1. — 340 с.
7. Криминалистика : учебник для вузов / под общ. ред. А. Г. Филиппова. — 4-е изд., перераб. и доп. — М. : Высшее образование, 2017. — 835 с.
8. Криминалистика : учебник для студентов вузов / под ред. А. Ф. Волынского, В. П. Лаврова. — 2-е изд., перераб. и доп. — М. : Юнити-Дана: Закон и право, 2008. — 943 с.
9. *Куроуз Д.*, *Росс К.* Компьютерные сети: нисходящий подход. — 6-е изд. — М. : Э, 2016. — 912 с.
10. *Россинская Е. Р.* Концепция частной криминалистической теории «информационно-компьютерное обеспечение криминалистической деятельности» // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIII Международной научно-практической конференции : в 2 т. — Иркутск : Восточно-Сибирский институт МВД РФ, 2018. — С. 113—118.
11. *Россинская Е. Р.* Криминалистика : учебник для вузов. — М. : Норма: Инфра-М, 2016. — 464 с.
12. *Торичко Р. С.*, *Клишина Н. Е.* Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. — 2018. — № 3. — С. 179—184.
13. *Чекунов И. Г.*, *Рядовский И. А.*, *Иванов М. А.* [и др.]. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / под ред. И. Г. Чекунова. — М. : Московский университет МВД России имени В. Я. Кикотя, 2018. — 106 с.
14. *Чекунов И. Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. — 2012. — № 1. — С. 9—22.
15. *Чулахов В. Н.* Криминалистическое учение о навыках и привычках человека : монография / под ред. Е. Р. Россинской. — М. : Юрлитинформ, 2007. — 284 с.
16. *Ligh M.*, *Adair S.*, *Hartstein B.*, *Richard M.* Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. — Indianapolis : Wiley Publishing, Inc., 2010. — 716 p.
17. *Matrosov A.*, *Rodionov E.*, *Bratus S.* Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. — No Starch Press, 2015. — 504 p.

Материал поступил в редакцию 12 января 2019 г.

MODERN MEANS OF COMMITTING COMPUTER CRIMES AND PATTERNS OF THEIR EXECUTION[25]

ROSSINSKAYA Elena Rafailovna, Doctor of Law, Professor, Director of the Forensic Examination Institute, Head of the Department of Forensic Examination of the Kutafin Moscow State Law University (MSAL), Honored Scientist of the Russian Federation, Honorary Worker of Higher Professional Education of the Russian Federation
elena.rossinskaya@gmail.com
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

RYADOVSKIY Igor Anatolevich, Head of Department of Investigation of Computer Incidents of JSC "Kaspersky Lab", Honorary Worker of Prosecutor's Office of the Russian Federation
igor.ryadovsky@kaspersky.com
125212, Russia, Moscow, Leningradskoe shosse, d. 39a, stroenie 3

Abstract. *The paper notes that the integration of modern information technologies in all spheres of human activity has led to the informatization and computerization of crime, when it is possible to commit almost any crime by means of computer tools and systems. There is a commonality of some elements of the mechanism of computer crimes, including information about the methods of these crimes.*
Means of committing computer crimes are considered from the standpoint of a new private theory of information and computer support of forensic activities, the subject of which are the laws of occurrence, movement, collection and study of computer information in the investigation of crimes. The objects are computer tools and systems, especially forensic technologies of collection (detection, fixation, seizure) and research of these objects to obtain evidence and guidance information. From the modern point of view, the method of crime is determined by personality, subject and circumstances of the criminal attack, the system of actions of the subject, aimed at achieving the criminal goal and united by a single criminal plan. The means of a crime commitment are divided into fully structured, including preparation, commission and concealment, and incomplete, when one or two elements are absent. The formation of the means of a crime is influenced by objective and subjective factors, which determines the determinism and repeatability of the means of the crime.
The main means of computer crimes are considered: aimed at hiding unauthorized access to computer tools and systems; the use of Trojans for various purposes; infection of computer systems with viruses; the use of hardware and software systems for mass campaigns of malicious software distribution to mobile devices; computer attacks on local corporate networks, etc.
It is established that the criminalistic regularity of the formation and implementation of computer crimes is a mandatory stage of preparation for the crime, which at the same time includes actions to conceal the traces of the crime, i.e. the methods of computer crimes are fully structured.

Keywords: *information and computer security, computer abuse, mechanism of a crime, means of crime commission, full structured means, incomplete means, malware, unauthorized access, Bootkit technology, Rootkit technologies, "disembodied" technology, encryption technology, obfuscation technology, Trojan, worm program, program-virus, bot-farm, local network attack.*

REFERENCES

1. Averyanova T.V., Belkin R.S., Korukhov Yu.G., Rossinskaya E.R. Kriminalistika: uchebnik dlya vuzov [Criminalistics: A Textbook for Universities]. 4th edition, rev. and suppl. Moscow: Norma Publ.: Infra-M, 2014. 928 p.
2. Belkin R.R. Kurs kriminalistiki [Course of Criminalistics]. 3 ed., suppl. Moscow: Yuniti-Dana Publ., Zakon i Pravo, 2001. 837 p.

[25] The study was carried out with the financial support of the Russian Foundation for Basic Research in the framework of the research project No. 18-29-16003/18.

3. Zuykov G.G. *«Modus operandi», kibernetika, poisk* ["Modus operandi", Cybernetics, Search]. *Kibernetika i pravo* [Cybernetics and law]. 1970. Pp. 46—56.
4. Zuykov G.G. *Kriminalisticheskoe uchenie o sposobe sovershenіya prestupleniya: avtoref. dis. … d-ra yurid. nauk* [Forensic doctrine of the method of committing a crime : Abstract of the Doctoral Degree Thesis. Moscow: Higher School of the USSR Interior Ministry, 1970. 31 p.
5. Zuykov G.G. *Kriminalisticheskoe uchenie o sposobe sovershenіya prestupleniya* [Forensic doctrine of the method of committing a crime]. Glava 6. Kriminalistika [Ch. 6. Criminology]. Edited by R.S. Belkin, I.M. Luzgin. Moscow: The Academy of the USSR Interior Ministry, 1978. Vol. 1. 384 p.
6. Zuykov G.G. *Osnovy kriminalisticheskogo ucheniya o sposobe sovershenіya i sokrytiya prestupleniya* [Fundamentals of forensic doctrine of the method of commission and concealment of the crime]. Glava 3. Kriminalistika: uchebnik dlya yuridicheskikh vuzov MVD SSSR [Chapter 3. Forensic Science : A Textbook for Law Schools of the USSR Interior Ministry. Edited by R.S. Belkin, V.P. Lavrov, I.M. Luzgin. Moscow: The Academy of the USSR Interior Ministry, 1987. Vol. 1. 340 p.
7. Kriminalistika: uchebnik dlya vuzov [Criminalistics : A Textbook for universities]. Edited by A.G. Filippov. 4th ed., rev. and suppl. Moscow: Vysshee obrazovanie Publ., 2017. 835 p.
8. Kriminalistika: uchebnik dlya vuzov [Criminalistics : A Textbook for students]. Edited by V.P. Lavrov. 2nd ed., rev. and suppl. Moscow: Yuniti-Dana Publ.: Law and Rights, 2008. 943 p.
9. Kurouz, D., Ross K. Kompyuternye seti: niskhodyashchiy podkhod [Computer network: top-down approach]. 6th ed. Moscow : E Publ., 2016. 912 p.
10. Rossinskaya E.R. *Kontseptsiya chastnoy kriminalisticheskoy teorii «informatsionno-kompyuternoe obespechenie kriminalisticheskoy deyatelnosti»* [Concept of private criminalistic theory "information and computer support of criminalistic activity"]. Deyatelnost pravookhranitelnykh organov v sovremennykh usloviyakh: Sbornik materialov xxiii mezhdunarodnoy nauchno-prakticheskoy konferentsii [Activity of law enforcement agencies in modern conditions : Proc. of the 23 International Scientific and Practical Conference : in 2 vols. Irkutsk: East Siberian Institute of the RF Ministry of Internal Affairs, 2018. Pp. 113—118.
11. Rossinskaya E.R. Kriminalistika: uchebnik dlya vuzov [Criminalistics: A Textbook for universities]. Moscow: Norma Publ.: Infra-M, 2016. 464 p.
12. Torichko R.S., Klishina N.E. *Nekotorye voprosy sovershenstvovaniya deystvuyushchego zakonodatelstva, reglamentiruyushchego rassledovanie kiberprestupleniy* [Some issues of improvement of the current legislation regulating the investigation of cybercrime]. *Vestnik ekonomicheskoy bezopasnosti* [Vestnik of Economic Security]. 2018. No. 3. Pp. 179—184.
13. Chekunov I.G., Ryadovskiy I.A., Ivanov M.A. [et al.]. Metodicheskie rekomendatsii po rassledovaniyu prestupleniy v sfere kompyuternoy informatsii: uchebnoe posobie [Guidelines for the investigation of crimes in the field of computer information : A Study Guide]. Edited by G.I. Chekunov. Moscow: Moscow University of the the Ministry of the Interior of Russia named after V. J. Kikot, 2018. 106 p.
14. Chekunov I.G. *Sovremennye kiberugrozy. Ugolovnopravovaya i kriminologicheskaya klassifikatsiya i kvalifikatsiya kiberprestupleniy* [Modern cyber threats. Criminal law and criminological classification of cybercrime]. *Pravo i kiberbezopasnost* [Law and cybersecurity]. 2012. No. 1. Pp. 9—22.
15. Chulakhov V. N. *Kriminalisticheskoe uchenie o navykakh i privychkakh cheloveka: monograph* [Criminalistic doctrine on the skills and habits of the person: the monograph]. Edited by E.R. Rossinskaya. Moscow: Yurlitinform Publ. 284 p.
16. Ligh M., Adair S., Hartstein B., Richard M. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Indianapolis: Wiley Publishing, Inc., 2010. 716 p.
17. Matrosov A., Rodionov E., Bratus S. Rootkits and Bootkits: Reversing Modern Malware and Next Generation threads. No Starch Press, 2015. - 504 p.