УДК 343.983

В.В. Поляков, С.А. Лапин

Средства совершения компьютерных преступлений

С криминалистических позиций исследованы средства совершения компьютерных преступлений. Предложено их классифицирование по существенно различным критериям: по законности происхождения; по созданию; по техническому содержанию; по технологии использования; по стадии в преступлении. Типизация данных о средствах совершения компьютерных преступлений позволяет установить корреляционные связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

Ключевые слова: средства совершения компьютерных преступлений, расследование компьютерных преступлений, криминалистика.

Быстрое развитие компьютерных технологий сопровождается ростом компьютерной преступности и, что еще более важно, ее качественным изменением. Преступления совершаются более изощренными способами с применением специальных программно-аппаратных средств и сетевых технологий. Способы совершения компьютерных преступлений становятся высокотехнологичными за счет применения нетривиальных технических решений, а также принципиально новых или модифицированных программ [1]. Преступники творчески используют и модифицируют компьютерную технику и программное обеспечение. Результатом таких действий становится исключительно высокая латентность компьютерных преступлений [2].

Вопрос о средствах совершения компьютерных преступлений, рассматриваемых с криминалистических позиций, является малоизученным. От современной криминалистики требуется изучение причин, благодаря которым компьютерные преступления становятся возможными, анализ применяемых преступниками технологий, аппаратных и программных средств подготовки, совершения и сокрытия преступлений. Эти вопросы входят в криминалистическую характеристику компьютерных преступлений и являются предметом доказывания по данной категории уголовных дел. В настоящей работе проводится анализ средств совершения компьютерных преступлений и предлагается их возможная криминалистическая классификация.

Преступления в сфере компьютерной информации всегда совершаются с помощью средств компьютерной техники. Понятие этих средства является комплексным, включающим в себя компьютеры в различных вариантах их исполнения (ноутбуки, планшеты, смартфоны, и т.д.), компьютерные технологии (беспроводные Wi-Fi, Bluetooth, 3G, WiMAX и др.), а также компьютерное программное обеспечение, находящееся в открытом, запрещенном или ограниченном обороте и имеющее различное назначение (разрешенные и бесплатно распространяемые программы, например, Opera, Mozilla Firefox, вредоносные программы, например, SpyEye, Zeus, Carberp и т.д.). Следует отметить, что в настоящее время главную роль при совершении компьютерных преступлений выполняет программное обеспечение, а не аппаратные средства, которые сами по себе обычно не представляют опасности.

Как показывает современная практика, в большинстве случаев компьютерные преступления совершаются путем удаленного доступа по телекоммуникационным сетям с помощью обычной компьютерной техники, на которую устанавливается специальное программное обеспечение [3]. Это принципиальное обстоятельство имеет следствия, исключительно важные как для расследования, так и для предотвращения компьютерных преступлений. Так, в непосредственных (бессетевых) способах совершения преступлений аппаратные средства, например аппаратные кейлогеры или скиммеры для негласного съема информации, действуют лишь в отношении конкретного компьютерного устройства. Преступники хорошо знают, что при совершении преступления непосредственным образом остаются традиционные (материальные) следы, по которым можно будет их идентифицировать. Использование вредоносного программного обеспечения при удаленном доступе по информационным сетям позволяет осуществить преступление одновременно в отношении многих компьютеров. При таком доступе преступникам не нужно проникать в помещение, в котором нахо-

дится объект посягательства, при этом остаются не персонифицируемыми их электронно-цифровые следы. Электронно-цифровые следы всегда образуются и модифицируются в результате опосредованного воздействия компьютерных программ. Специфика этих следов проявляется в том, что они не имеют геометрической формы, цвета, запаха и иных характеристик, традиционно рассматриваемых криминалистикой, в которых могли бы отразиться отельные черты преступника, например его ДНК, запах, папиллярный узор и т.д. Таким образом, в механизме следообразования нет непосредственного следового контакта с преступником, его физическими и иными особенностями, так как компьютерная программа не несет на себе отпечатка конкретного человека, одни и те же электронно-цифровые следы-последствия могут быть образованы кем угодно. Несмотря на эту специфику, основным источником информации о средствах, применяемых в компьютерном преступлении, остаются именно конкретные следы и вся следовая картина в целом.

В настоящее время для совершения большинства компьютерных преступлений не требуется наличия средств преступления в виде дорогостоящей компьютерной техники. Практически каждый может найти в сети Интернет бесплатные вредоносные программы, включающие в себя необходимый для совершения преступления алгоритм действий. К таким программам могут прикладываться наглядные инструкции по их использованию. Эти обстоятельства в значительной степени способствуют росту числа совершаемых преступлений в сфере компьютерной информации [4]. Более того, помимо количества преступлений, меняется типичный портрет преступника в сторону лиц, не имеющих специального или высшего образования и постоянной работы [5–8].

Следственные органы, особенно на первоначальном этапе расследования компьютерных преступлений, редко располагают сведениями о средствах, используемых в преступлении. В отсутствие такой информации имеет важную роль для проведения расследования криминалистическая характеристика аналогичных преступлений. Ее практическое значение, проявляющееся в корреляционной взаимосвязи между структурными элементами преступления, дает основания строить следственные версии на основе использования имеющихся неполных данных. В компьютерных преступлениях выбор средств для их совершения обычно зависит от целого ряда факторов: объекта посягательства, принятого на нем режима охраны, применяемых технических и организационных средств охраны, программно-аппаратной защиты информации. Так как в большинстве случаев поводом для возбуждения уголовных дел являются заявления потерпевших, то следствию становится известен объект посягательства. Его исследование может пролить свет на способ совершения преступления или примененные преступником программно-аппаратные средства. Анализ судебно-следственной практики показывает, что типичные (относительно простые) или, наоборот, высокотехнологичные способы совершения преступлений могут осуществляться характерными для них программно-аппаратными средствами. Возможна также обратная ситуация, когда данные о средствах преступления известны и помогают строить следственные версии о других искомых элементах преступления. Например, конкретные средства совершения преступления могут указывать на применяемый преступниками способ совершения преступления, а также время и место его осуществления.

Средства, которые используются при совершении преступлений в сфере компьютерной информации, достаточно разнообразны. Важно также, что с криминалистических позиций их можно классифицировать по существенно различным критериям: по законности происхождения; по созданию; по техническому содержанию; по технологии использования; по стадии в преступлении и др. Это обусловливает необходимость разработки системы криминалистической классификации. В целях повышения эффективности расследования компьютерных преступлений разнообразные средства их совершения следует классифицировать, учитывая их основные особенности (таблица).

Как следует из таблицы, средства, предназначенные для полного или частичного управления компьютером и доступа к хранимой на нем информации предлагается прежде всего разграничить на две основные группы – законные и незаконные. Законные (разрешенные для использования) средства могут быть свободно распространяемыми, находиться в ограниченном обороте или быть изъятыми из оборота. Некоторые такие программные средства могут входить в состав операционной системы или устанавливаться самими пользователями дополнительного. Ограниченные в гражданско-правовом обороте средства, например, предназначенные для негласно получения информации путем видеоаудиозаписи, могут быть приобретены при наличии соответствующего разрешения. Использование изъятых из оборота специальных средств может быть разрешено органам оперативно-розыскной деятельности или иным государственным органам (например, следственному коми-

тету, прокуратуре, суду, экспертным учреждениям), однако создавать, владеть, пользоваться и распоряжаться такими средствами гражданам запрещено законом, т.е. их использование гражданами является незаконным.

Криминалистическая классификация средств совершения компьютерных преступлений

По законности происхождения		По созданию			По техническому содержанию			По технологии использования		По стадии в преступлении			
Законные	Незаконные	Готовые	Модифицированные	Собственной разработки	Аппаратные	Программно-аппаратные	Программные	Без удаленного доступа	С удаленным доступом	При подготовке	При совершении	При сокрытии	При противодействии следствию

Преступниками может применяться не только широкий перечень готового программно-аппаратного обеспечения, в том числе модифицированного, но и собственные уникальные разработки. Это наиболее характерно для высокотехнологичных способов совершения компьютерных преступлений, при которых используются компьютерные программы, созданные членами преступной группы или посторонними специалистами по заказу преступников. В этом случае речь идет прежде всего о так называемых шеллах (shell), которые позволяют преступнику выполнять ограниченный круг команд по управлению автоматизированным рабочим местом (например, выполнить какое-либо действие командной оболочки операционной системы и т.п.).

По техническому содержанию рассматриваемые средства могут быть условно разделены на аппаратные, программные и программно-аппаратные. При незаконном доступе к объекту посягательства использование чисто аппаратных средств мало распространено, так как современные компьютерные устройства обычно обладают каким-либо собственным программным обеспечением. Как показывает судебно-следственная практика, примерами программно-аппаратных устройств выступают скиммеры и кейлогеры. Скиммеры используют для кражи реквизитов банковских карт. Как правило, скиммер состоит из двух компонентов – устройства для считывания данных хранящейся на магнитной полосе банковской карты и устройства, позволяющего скопировать пин-код. Некоторые скиммеры оснащены инструментами беспроводной связи, с помощью которой злоумышленники получают информацию в реальном времени, а не хранят ее непосредственно на скиммере. Кейлогеры представляют собой устройства, которые позволяют перехватывать данные, вводимые с клавиатуры. Они выполняются в различных вариантах и могут хранить полученную информацию в собственной памяти или быть оснащены средствами беспроводной связи. Программное обеспечение, используемое для незаконного доступа к компьютерной информации, может быть признано вредоносным только судом. Отметим, что четкого определения вредоносного программного обеспечения в ст. 273 УК РФ не дается, что требует отдельного рассмотрения.

При проведении расследовании целесообразно учитывать, что конкретные средства совершения компьютерных преступлений могут использоваться только на определенных стадиях – подготовки к преступлению, непосредственно при его совершении, при сокрытии преступления, при противодействии следствию в условиях оперативно-розыскных мероприятий или следственных действий. Так, на стадии подготовки преступники изучают обстановку объекта посягательства, физический режим его охраны (замки, контроль сотрудниками, видеонаблюдение, сигнализацию), пытаются собрать информацию о действующих устройствах и программах информационной безопасности (системах идентификации и аутентификации), готовят хранилища для переноса охраняемой информации (flash носители, облачные хранилища и пр.), средства сокрытия и уничтожения следов своей деятельности (например, размагничивание жесткого диска). На этой стадии могут применяться специальные программы, исследующие и оценивающие объект посягательства с точки зрения его защищенности внешним угрозам (например, программы-шпионы типа Zeus). Непосредственно на этапе совершения преступления соответствующие средства направлены на получение преступником возможности управлять автоматизированным рабочим местом потерпевшего. Для получения неправомерного доступа преступники могут использовать программы, предназначенные для администраторов (TeamViewer, Radmin, TightVNC и т.п.), специализированные клиенты сетевых протоколов RDP (Remote Desktop Protocol) или VNC (Virtual Network Computing), имеющие собственный web-интерфейс для администрирования и управления, либо модификации вредоносного программ-

ного обеспечения, например Zeus, Carberp и т.п. Опасной разновидностью вредоносного программного обеспечения, позволяющего получить неправомерный доступ к автоматизированному рабочему месту, являются эксплойты, под которыми понимается программный код или его фрагмент, который через ошибки в каком-либо программном обеспечении, работающем на объекте посягательства, приводит к выполнению этим программным обеспечением действия, непредусмотренного разработчиками. При попытке массового заражения рабочих мест через использование web-сервисов применяются инструменты, которые включают в себя наборы эксплойтов, нацеленные на эксплуатацию ошибок в web-браузерах и различного рода расширений к ним (Adobe Flash, ActiveX и т.п.).

Сокрытие преступления, отдельных следов-последствий и участия в нем преступника может реализовываться во время совершения преступления и после него. Для этой цели могут применяться различные элементы маскировки, например: программно-аппаратный сбой, противоправные действия иных лиц и многое другое. Отметим, что для сокрытия электронно-цифровых следов может применяться не только вредоносное, но и законное программное обеспечение, например, позволяющее безвозвратно удалять информацию с носителя путем многократной ее перезаписи. Как правило, сокрытие сводится к попытке затруднить определение местонахождения преступников. Подобная цель может достигаться путем использования сервисов, позволяющих осуществить подмену реального IP-адреса на другой. Популярностью у преступников пользуются услуги предоставления доступа к сети, работающей по протоколу VPN. Современные VPN-сервисы предоставляют доступ к сети путем использования цепочки промежуточных серверов (Double/Triple-VPN), что значительно затрудняет определение реального IP-адреса преступника. В случаях, когда не требуется высокая пропускная способность канала связи, преступник может отдать предпочтение таким технологиям, как Tor, ввиду бесплатного предоставления анонимности при работе в телекоммуникационных сетях.

Исследование средств совершения компьютерных преступлений с позиций криминалистики, их типизация и классификация позволяют установить корреляционные связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

Работа выполнена по гранту Президента Российской Федерации для государственной поддержки молодых российских ученых МК7026.2013.6.

Литература

1. Поляков В.В. Характеристика высокотехнологичных способов совершения преступлений в сфере компьютерной информации: матер. ежег. Всерос. науч.-практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета «Уголовно-процессуальные и криминалистические чтения на Алтае». – Барнаул: Изд-во Алт. ун-та, 2012. – Вып. 11–12. – С. 123–126.
2. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. – № 24. – С. 43–46.
3. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114–116.
4. Internet security threat report 2013 [Электронный ресурс]. – Режим доступа: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf, свободный (дата обращения: 01.05.2014).
5. Уголовное дело № 706/09 // Архив Железнодорожного районного суда г. Барнаула. – 2009.
6. Уголовное дело № 1-179/06 // Архив суда г. Алейска. – 2006.
7. Уголовное дело № 1-337/2011 // Архив суда г. Новоалтайска. – 2011.
8. Уголовное дело № 2-23/2011 // Архив суда г. Камень-на-Оби. – 2011.

Поляков Виталий Викторович
Канд. юрид. наук, доцент каф. уголовного процесса и криминалистики
Алтайского государственного университета (АлтГУ)
Тел.: 8 (385-2) 36-64-52
Эл. почта: vvpagu@rambler.ru

Лапин Сергей Александрович
Аспирант каф. прикладной физики, электроники и информационной безопасности АлтГУ
Тел.: 8 (385-2) 36-40-65
Эл. почта: lapinsa567@gmail.com

Polyakov V.V., Lapin S.A.
Means of committing computercrimes

In this paper means of committing computer crimes were investigated dealing with criminalistics. Autor made classification for their different criteria: legal emergence; development; technical content; technology use; stages of the crime. Typing information about means of committing computer crimes makes correlation between the established circumstances and evidence in the criminal cases. It can raise the effectiveness of the investigation of such crimes.
Keywords: means of committing computer crimes, computer crime investigation, criminalistics.