Пихачева Ольга Олеговна

Магистрант

Направление: Юриспруденция

Магистерская программа: Уголовное право, криминология, уголовно-исполнительное право

Средства совершения компьютерных преступлений

Аннотация. 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.

Ключевые слова: уголовный процесс, криминалистика, методика расследования компьютерных преступлений, средства совершения компьютерных преступлений.

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.

Преступления в сфере компьютерной информации всегда совершаются с помощью средств компьютерной техники. Понятие этих средств 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.) [2, с. 20].

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 [3, с. 87].

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 техни-

ческому 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 (табл. 1).

Таблица 1

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

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

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 [1, с. 114].

Литература

1. Вехов В.Б. Компьютерные преступления: Способы совершения, методики расследования. М.: Право и закон, 2010.

2. Иванов А., Силантьев Д. Выемка электронной почты в сети Интернет // Законность. 2012. № 5.

3. Крылов В.В. Информационные компьютерные преступления. М.: Норма, 2011.