УДК 343.91: (575.2) (04)

# КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА СПОСОБОВ СОВЕРШЕНИЯ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В СЕТЯХ ЭВМ

***Э.А. Ли*** *– с*оискатель

This article is devoted to the methods of commission of illegal access to computer information in computer networks on the basis of the used materials it is urgent and completely reflects the involved topic. Intense development and wide implementation of the computer digital techniques means and high tech result in increase of crimes in the sphere of computer information's motion what concentrated attention on the lack of serious scientific investigations in this field in the Kyrgyz Republic. Criminalistic analysis of methods of commission of illegal access to computer information in computer networks that has both theoretical and applied meaning is done in this article. The aim of research is rendering of assistance to the law machinery in knowledge increasing and implementation of scientific workings in prevention, disclosure and investigation of illegal access to computer information in computer networks.

Способ совершения преступления в криминалистике представляет собой систему взаимообусловленных, подвижно детерминированных действий, направленных на подготовку, совершение и сокрытие преступления, связанных с использованием соответствующих орудий и средств, а также времени, места и других способствующих обстоятельств объективной обстановки совершения преступления[1].

Способ совершения компьютерного преступления играет определяющую роль в формировании информации о содеянном и лице, его совершившем. Так, Н.П. Яблоков указывал, что в криминалистическом смысле важно, чтобы преступник оставил как можно больше следов, позволяющих судить о деталях его поведения и тех объективных и субъективных факторах, которые его обусловили[2].

Систематизацией способов совершения преступлений в сфере компьютерной информации занималось множество ученых, в том числе: Б.Х. Толеубекова, В.Б. Вехов, Ю.М. Батурин, В.В. Крылов и др[3].

Проанализировав точки зрения ученых по вопросу классификации способов совершения преступлений в сфере компьютерной информации, можно прийти к выводу, что, несмотря на многообразие способов преступных посягательств и их классификацию, все способы совершения данного вида преступлений можно сгруппировать в несколько основных блоков. В данном случае, мы будем придерживаться классификации элементов способов совершения

[1] *Зуйков Г.Г.* Установление способа совершения преступления. – М.: МВШ МВД СССР, 1970. – С. 15–16.

[2] *Васильев А.Н., Яблоков Н.П.* Предмет, система и теоретические основы криминалистики. – М.: МГУ, 1984. – С. 119.

[3] *Толеубекова Ю.Х.* Компьютерная преступность: уголовно-правовые и процессуальные аспекты. – Караганда: КВШ МВД СССР, 1991. – С. 18.

преступлений в сфере компьютерной информации, приведенной В.Е. Козловым, так как она с наибольшей точностью обобщает все способы совершения преступлений, которыми являются:

- несанкционированный доступ;
- злонамеренная вирусная модификация;
- перехват информации;
- комбинированное использование способов[1].

В свою очередь несанкционированный доступ к компьютерной информации включает такие элементы, как несанкционированные подключение, копирование, модификация, блокирование, уничтожение.

Под несанкционированным подключением мы понимаем самовольное подключение к информационным ресурсам и сетей ЭВМ, путем программного или аппаратного, контактного или бесконтактного внедрения в различного рода передающие линии как физические, так и виртуальные. Эти цели достигаются при помощи различных технических средств. В специальной литературе описаны также и некоторые иные разновидности несанкционированных подключений[2]:

- считывание данных в массивах других пользователей;
- считывание остаточной информации в памяти системы после выполнения санкционированных запросов;
- маскировка под зарегистрированного пользователя;
- маскировка под запросы системы в форме несанкционированного подключения с воздействием на парольно-ключевые системы средства электронной защиты;
- иные.

Под копированием информации понимается воспроизведение точного или относительно точного ее оригинала[3].

При совершении криминальных действий, связанных с несанкционированным копированием информации, преступники, как правило, копируют:

- документы, содержащие интересующую их информацию;
- технические носители;
- информацию, обрабатываемую в информационных системах.

Даже незначительная модификация программ в автоматизированных информационных системах может обеспечить преступнику возможность несанкционированного доступа к информации. Что касается термина "модификация информации", следует отметить, что исследователи едины в его толковании.

Под модификацией информации некоторые авторы понимают внесение в нее любых изменений, обусловливающих ее отличие от той, которую включил в систему и которой владеет собственник информационного ресурса[4]. Другие – конкретизируют термин "модификация информации" как ее видоизменение, характеризующееся появлением новых, нежелательных свойств. Как правило, несанкционированное подключение сопровождается несанкционированной модификацией файлов данных. Существуют примеры модификации и прикладного программного обеспечения.

Несанкционированное блокирование информации заключается в невозможности доступа к ней со стороны законного пользователя. Некоторые исследователи склонны к большей конкретизации данного термина, определяя блокирование как "результат воздействия на ЭВМ и ее элементы, повлекшего временную или постоянную невозможность осуществлять какие-либо операции над компьютерной информацией"[5].

Механизмы воздействия на информационные и технологические процессы, а также последствия применения блокирования довольно сложны, однако чаще всего блокирование проявляется в виде остановки (так называемое "зависание") ЭВМ.

Несанкционированное уничтожение компьютерной информации понимается исследова-

---

[1] *Козлов В.Е.* Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия – Телеком, 2002. – С. 127.

[2] *Леонов А.П., Леонов К.А., Фролов Г.В.* Безопасность автоматизированных банковских систем. – Минск: НКП Беларуси, 1996. – С. 33.

[3] Руководство для следователей / Под. ред. Н.А. Селиванова, В.А. Снеткова. – М.: Новый юрист, 1997. – С. 655.

[4] *Крылов В.В*. Информационные компьютерные преступления. – М.: ИНФА-М-НОРМА, 1997. – С. 49.

[5] Там же. – С. 52.

телями-криминалистами либо как “полная физическая ликвидация информации или ликвидация таких ее элементов, которые влияют на изменение существенных идентифицирующих информацию признаков”, либо как “такое изменение ее состояния, при котором она лишается своей первоначальной, качественной определенности и перестает отвечать своему назначению”[1].

Содержание понятия “несанкционированное уничтожение компьютерной информации” нуждается в расширении. Как известно, информация в ЭВМ хранится в виде файлов, размещенных на носителях. Поэтому уничтожение может осуществляться как информационных или программных файлов, так и носителей искомой информации. Таким образом, несанкционированным уничтожением компьютерной информации мы предлагаем считать полную или частичную физическую ликвидацию как самой информации, так и ее машинных и иных оригинальных носителей, при котором ее дальнейшая обработка при помощи ЭВМ затруднена либо невозможна.

Данная разновидность способа совершения компьютерных преступлений представляет особую опасность для автоматизированных систем, в которых накапливаются на технических носителях огромные объемы сведений различного характера. Информация на магнитных носителях может быть уничтожена умышленными или неосторожными действиями лиц, имеющих возможность воздействия на эту информацию программным путем, с помощью магнитного излучения, с использованием иных специально приспособленных средств.

Под перехватом понимают получение разведывательной информации путем приема электромагнитного и акустического излучения пассивными средствами приема, расположенными, как правило, на безопасном расстоянии от источника информации[2].

Исследователи-криминалисты по-иному классифицируют способы ведения перехвата. Так, В. Б. Вехов выделяет:

- непосредственный перехват;
- форсированный перехват;
- перехват символов;
- перехват сообщений[3].

Мы считаем, что с точки зрения расследования гораздо важнее знать информацию о механизме подключения устройств дистанционного съема информации, так как эти сведения позволяют определенно судить о квалификации лиц, ведущих радиоэлектронную разведку, характере связей с пострадавшим от компьютерных преступлений субъектом хозяйствования.

Установление факта применения перехвата имеет особое значение при рассмотрении обстоятельств подготовки к совершению компьютерного преступления. Являясь способом ведения разведывательной деятельности, перехват информации с помощью технических средств связан с “подслушиванием” содержания передаваемой информации и извлечением соответствующих данных напрямую, через доступ и использование компьютерной системы, либо косвенно, путем использования электронных подслушивающих или записывающих устройств. Например:

- перехват информации в технических каналах возможной утечки ее;
- перехват информации посредством внедрения электронных устройств в помещении;
- радиоэлектронное подавление линий связи и систем управления.

Ведение радиоэлектронной разведки возможно путем перехвата открытых и кодированных систем и линий связи, например, возможно выявление паролей в компьютерной сети, перехват электромагнитных сигналов, возникающих в электронных средствах за счет самовозбуждения, акустического воздействия, паразитных колебаний, излучений монитора ЭВМ, возникающих при выводе информации на экран электронно-лучевой трубки.

Для анализа сохранной информации в стационарных условиях возможно использование преступниками видеомагнитофонов. Перехвату подвержены передачи данных и переговоры с радиомодемов и радиотелефонов.

[1] Руководство для следователей / Под. ред. Н.А. Селиванова, В.А. Снеткова.– М.: Новый юрист, 1997. – С. 655.

[2] *Леонов А.П., Леонов К.А., Фролов Г.В.* Указ. соч. – С. 211.

[3] *Вехов В.Б.* Компьютерные преступления. Способы совершения, методики расследования. – М.: Право и закон, 1996. – С. 57.

С криминалистической точки зрения под злонамеренной вирусной модификацией мы понимает разработку, использование либо распространение таких программ, которые заведомо приводят к нарушению работы ЭВМ или их сетей, внесению несанкционированных собственником изменений в компьютерную информацию. При этом большинство исследователей в области безопасности компьютерных систем сходятся во мнении, что под распространением понимают расширение сферы применения таких программ за пределы рабочего места их создателя[1].

Существует множество типов вирусов, каждый из которых обладает собственными отличительными признаками. Для классификации данного способа совершения компьютерного преступления целесообразно установить последствия действий вредоносных программ, их наиболее яркие проявления. Существование физического неправомерного доступа к компьютерной информации в сетях, как способа проникновения является достаточно спорным и, по нашему мнению, к нему следует относиться крайне осторожно. Данные действия могут являться как самостоятельным преступлением со своей уголовно-правовой квалификацией, так и разновидностью способа неправомерного доступа к компьютерной информации в сетях ЭВМ на различных стадиях совершения преступления. Но физический доступ никак нельзя считать оконченным компьютерным преступлением.

Логический несанкционированный доступ предполагает логическое преодоление системы защиты ресурсов активной компьютерной сети.

По положению источника несанкционированного доступа различают несанкционированный доступ, источник которого расположен в локальной и вне локальной сети.

В первом случае атака проводится непосредственно из любой точки локальной сети. Инициатором такой атаки чаще всего выступает санкционированный пользователь.

При подключении любой закрытой компьютерной сети к открытым сетям, например, Internet, высокую актуальность приобретают возможности несанкционированного вторжения в закрытую сеть из открытой (извне). Подобный вид атак характерен также для случая, когда объединяются отдельные сети, ориентированные на обработку конфиденциальной информации совершенно разного уровня секретности или разных категорий. При ограничении доступа этих сетей друг к другу возникают угрозы нарушения установленных ограничений.

По режиму выполнения несанкционированного доступа различают атаки, выполняемые при непосредственном участии человека, либо специально разработанными программами без участия человека.

В первом случае для воздействия на компьютерную систему может использоваться и стандартное программное обеспечение. Во втором случае всегда применяют специально разработанные программы, в основе функционирования которых – вирусная технология[2].

Анализируя и принимая во внимание мнение некоторых ученых, к типичным орудиям подготовки, совершения и сокрытия преступлений в сфере компьютерной информации можно отнести:

1. Средства ЭВМ:

- различные виды ЭВМ, их сети, предназначенные для автоматической обработки информации в процессе решения вычислительных и информационных задач;
- периферийные устройства – устройства, обеспечивающие передачу данных и команд;
- внешние носители информации (магнитные ленты, CD-диски, USB-дисководы, Flash-карты и т.п.);
- некоторые аппаратные средства (соединительные провода, шины, шлейфы, разъемы, “шнурки”, устройства электропитания и т.д.);
- устройства приема и передачи компьютерной информации (сетевое оборудование, модемы INT, EXT, ADSL, WI-FI и Bluetooth – оборудование, другие средства телекоммуникаций);

[1] *Ляпунов Б., Максимов В.* Ответственность за компьютерные преступления // Законность. – 1997. – №1. – С. 113.

[2] *Зима В.М., Молдовян А.А., Молдовян Н.А.* Безопасность глобальных сетевых технологий. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – С. 109.

- разработанные, приспособленные и запрограммированные специальные технические средства негласного получения информации.

2. ПО – программное обеспечение и специализированные программные средства (вредоносные программы для ЭВМ типа Троянский конь, Червь, и т.п., Remote Administrator).

3. Разнообразные магнитные материалы и специальные технические устройства, генерирующие направленное электромагнитное излучение.

4. Электромонтажный инструмент и материалы.

5. Контрольно-измерительные приборы и устройства.

Наиболее широко применяемым универсальным орудием совершения преступления в сфере компьютерной информации является персональная ЭВМ (ПЭВМ) или персональный компьютер (ПК) с соответствующим программным обеспечением, а также переносной диск с установленным программным обеспечением, которое активируется при подключении к ПК собственника информации.

Учитывая рост и развитие компьютерных технологий, при котором постоянно совершенствуются средства и орудия, используемые для неправомерного доступа к компьютерной информации в сетях ЭВМ, нельзя пренебрегать составлением четкого алгоритма действий сотрудников правоохранительных органов, а также программированием следственных действий при расследовании этой категории преступлений. Применение современных технических и программных средств позволит выявить и зафиксировать следы несанкционированного доступа, а правовое урегулирование отношений в сфере движения информации будет иметь практическую значимость по обеспечению безопасности в сетях ЭВМ и предупреждению неправомерного доступа к компьютерной информации.

Таким образом, представленная криминалистическая характеристика способов совершения неправомерного доступа к компьютерной информации в сетях ЭВМ поможет определить круг проблем выявления этих способов, что позволит сотрудникам правоохранительных органов иметь достаточное представление об уже изученных способах, эффективнее принимать меры по предупреждению в ходе раскрытия и расследования неправомерного доступа к компьютерной информации в сетях ЭВМ. Так, одной из основных задач нашего исследования является разработка и внедрение практических рекомендаций по алгоритмизации действий следователя при расследовании неправомерного доступа к компьютерной информации в сетях ЭВМ.