Дудова Татьяна Алексеевна
4 курс, юридический факультет
Российской таможенной академии

Следы компьютерных преступлений

Интенсивное развитие средств информатизации и телекоммуникаций, широкое их внедрение во все сферы человеческой деятельности привели к возникновению нового вида преступлений – преступлений в сфере компьютерной информации, или, как их нередко называют, компьютерных преступлений.

Объект данного исследования составляет деятельность следователей, сотрудников правоохранительных органов, направленная на выявление и расследование преступлений в сфере компьютерной информации.

Предметом работы является выявление и изучение механизмов образования следов, методы и приемы их обнаружения, фиксации и исследования.

Актуальность исследования данной проблемы и недостаточная ее разработанность (о чем скажем ниже) обусловливается также потребностями дальнейшего развития криминалистической теории, обогащения ее достижениями смежных наук и углубления научных знаний о методике расследования преступлений.

Одной из наименее исследованных проблем в данной области является проблема обнаружения и выявления следов компьютерных преступлений. Следы в сфере компьютерной информации в силу специфики рассматриваемого вида преступлений редко остается в виде изменения внешней среды. Они в основном не рассматриваются в современной трасологии, поскольку в большинстве случаев носят информационный характер, то есть представляют собой те или иные изменения в компьютерной информации, имеющие форму ее уничтожения, модификации, копирования, блокирования.

На основании изложенного представляется целесообразным эти следы разделить на два типа: традиционные следы (следы отображения, рассматриваемые трасологией, а также следы-вещества и следы-предметы) и нетрадиционные – информационные следы.

К первому типу относятся материальные следы. Ими могут являться какие- либо рукописные записи, распечатки и т.п., свидетельствующие о приготовлении и совершении преступления.

Информационные следы образуются в результате воздействия (уничтожения, модификации, копирования, блокирования) на компьютерную информацию путем доступа к ней и представляют собой любые изменения компьютерной информации, связанные с событием преступления. Прежде всего, они остаются на машинных носителях информации и отражают изменения в хранящейся в них информации. Речь идет о следах модификации информации, находящейся на жестких дисках ЭВМ, дискетах и иных материальных носителях. Кроме того, эти носители могут нести следы уничтожения и модификации информации. Данные следы могут быть выявлены при изучении компьютерного оборудования, рабочих записей программистов, протоколов работы антивирусных программ, программного обеспечения.

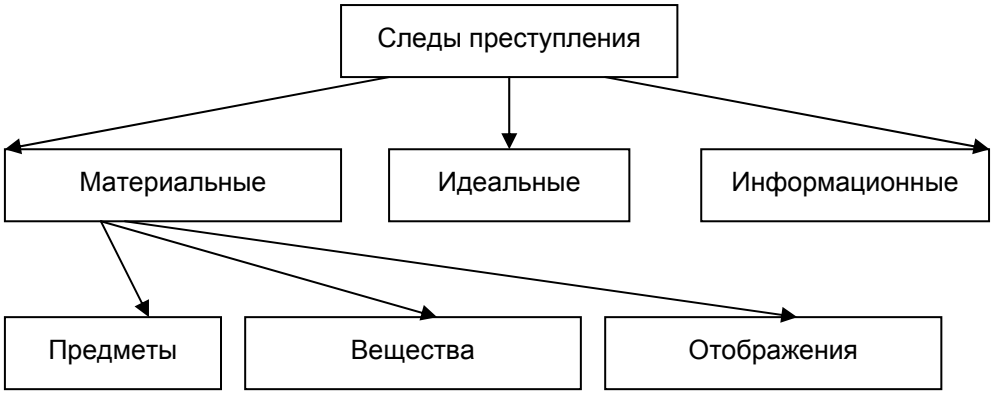
В нижепредставленной схеме отражено место информационных следов в криминалистической классификации.

Информационные следы могут оставаться и при опосредованном (удаленном) доступе через компьютерные сети (например, Интернет).

Следами, указывающими на посторонний доступ к информации, могут являться: переименование каталогов и файлов; изменение размеров и содержимого файлов, изменение стандартных реквизитов файлов, даты и времени их создания; появление новых каталогов и пр.

Перечисленное может свидетельствовать об изменениях в заданной структуре файловой системы, а также об изменении содержимого файлов.

Сборник конкурсных студенческих научных работ, посвященных 15-летию Федеральной таможенной службы, 10-летию Всероссийского Союза ветеранов таможенной службы Российской Федерации / Под общ. ред. К.А. Корнякова -М.: РИО РТА, 2006.



На неправомерный доступ к компьютерной информации могут указывать и необычные проявления в работе ЭВМ, как то: замедленная или неправильная загрузка операционной системы; замедленная реакция машины на ввод с клавиатуры; замедленная работа машины с дисковыми накопителями при записи и считывании информации; неадекватная реакция ЭВМ на команды пользователя и пр.

Одним из наиболее часто встречающихся в настоящее время видов преступлений в сфере компьютерной информации является распространение вредоносных программ. В.А. Мещеряков на примере данного вида преступлений рассмотрел особенности механизма образования "виртуальных" следов. Механизм следообразования – это специфическая конкретная форма протекания процесса, конечная фаза которого представляет собой образование следа-отображения. Элементами этого механизма являются объекты следообразования – следообразующий, следовоспринимающий, следовой контакт как результат взаимодействия вследствие приложения энергии к объектам следообразования[1]. В зависимости от этапа совершения данного вида преступления будет существовать различный набор следообразующих объектов. Например, на этапе внедрения известной программы "Троянский конь" это сообщение электронной почты с прикрепленным исполняемым файлом в специальном формате, а на этапе активизации к нему добавится еще исполняемый файл. При этом основными с криминалистической точки зрения характеристиками следообразующих объектов будут:

- размер программ и сообщения электронной почты с присоединенным файлом;
- дата и время создания/получения и/или модификации файлов и сообщения;
- отдельные атрибуты (например, признак архивного, скрытого или системного файла, уровень важности и конфиденциальности полученного сообщения) файлы и сообщения;
- характерные записи исполняемых программ или файлов конфигурации, позволяющие идентифицировать конкретный экземпляр вредоносной программы. Например, адрес электронного почтового ящика, куда следует отсылать выкраденные пароли, логины и IP- адреса компьютера.

Помимо самих файлов вредоносной программы следообразующими объектами также будут:

1. Файлы, использующиеся для электронной рассылки "троянских коней":

а) специализированная программа рассылки электронных сообщений (ее вид, версия, текущие настройки);
б) текстовые файлы или файлы в специальном формате, содержащие списки рассылки и вспомогательные данные – даты и время рассылки, количество попыток повторения и т.п.

2. Файлы компилятора, использующегося для создания (программирования или настройки) самой вредоносной программы:

а) версия, настройки и параметры. Эти данные в ряде компиляторов включаются в тело создаваемой с их помощью программы;

[1] Мещеряков В.А. Механизм следообразования при совершении преступлений в сфере компьютерной информации // Известия Тульского государственного университета. Серия: Современные проблемы законодательства России, юридических наук и правоохранительной деятельности. Вып. 3. Тула 2000 - с. 170-172.

б) используемые библиотеки компилятора, операционной системы или других пакетов прикладных программ. Ряд программ рассчитан на обязательное присутствие на компьютере отдельных библиотек или отдельных пакетов прикладных программ. Например, известны случаи, когда вредоносные программы типа "троянский конь" для рассылки украденной парольно-ключевой информации используют коммуникационные средства программы обмена информацией в реальном времени ICQ.

Учитывая, что при совершении рассмотренных выше преступлений в сфере компьютерной информации используется, по крайней мере, два компьютера (преступника и жертвы), то следовоспринимающих объектов также будет несколько.

На компьютере жертвы такими объектами будут:

1. Таблица размещения файлов. На компьютере жертвы должны появиться файлы с программами, представляющими собой часть вредоносной программы "троянский конь". Как правило, это два файла: один исполняемый файл (непосредственно сама программа), а второй файл содержит параметры конфигурации и вспомогательные данные, необходимые для работы исполняемого файла; Имена этих файлов могут быть произвольными (легко и без изменения функциональных возможностей программы заменяются преступником), но они должны иметь фиксированную (одну и ту же) длину, а также дата и время создания/модификации этих файлов должны соответствовать дате и времени установки этих программ на компьютер-жертву.
2. Системный реестр операционной системы. Соответствующие разделы системного реестра должны включать указания на размещение и параметры установленных программных файлов.
3. Отдельные кластеры магнитного носителя информации (винчестера, дискеты), в которых записываются фрагменты исполняемых файлов, конфигурации почтовой программы.
4. Файлы и каталоги (папки) хранения входящей электронной почты и прикрепленных исполняемых файлов, конфигурации почтовой программы.
5. Файлы конфигурации программ удаленного соединения компьютера с информационной сетью.

На компьютере преступника такими объектами будут:

1. Таблица размещения файлов. На компьютере жертвы должны появиться файлы с программами, представляющими собой вторую (управляющую) часть вредоносной программы "троянский конь".
2. Системный реестр операционной системы. Соответствующие разделы системного реестра должны включать указания на размещение и параметры установленных программных файлов.
3. Скопированные с компьютера-жертвы файлы данных и программы, а также так называемые "скриншоты" (графические изображения экрана монитора) с компьютера-жертвы.
4. Файлы и каталоги (папки) хранения входящей электронной почты, конфигурации почтовой программы. Здесь могут быть обнаружены присланные с компьютера-жертвы значения паролей и логинов для входа в информационную сеть, копии украденной электронной корреспонденции и т.п.
5. Файлы конфигурации программ удаленного соединения компьютера с информационной сетью. В этих файлах могут быть обнаружены логины и пароли компьютера-жертвы, его адресная книга, используемые скрипты и т.п.
6. Отдельные кластеры магнитного носителя информации (винчестер и дискеты), в которых записываются фрагменты исполняемых файлов (программ) и файлов конфигурации.

При современном развитии вычислительной техники и информационных технологий "компьютерные следы" преступной деятельности имеют широкое распространение. Это должно учитываться следователями и оперативными работниками в их деятельности по собиранию доказательств наряду с поиском уже ставших традиционными следов[2].

[2] Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: автореф. дисс... канд. юрид. наук. М. 1997. С. 14.

Типичными традиционными следами являются:

1. Следы орудий взлома, повреждения, уничтожения и (или) модификации охранных и сигнальных устройств.
2. Показания регистрирующей аппаратуры (видеотехники, электронного журнала учета операций с компьютерной информацией, доступа к ней и СВТ, др.).
3. Показания специальных мониторинговых (тестовых) программно-аппаратных средств, в том числе электронной цифровой подписи (сокр. ЭЦП); следы пальцев рук на СВТ, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, на розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих и отключающих СВТ и электрооборудование;
4. Остатки соединительных проводов и изоляционных материалов.
5. Капли припоя, канифоли или флюса; следы вдавливания, проплавления, прокола, надреза изоляции токонесущих и соединительных (управляющих) проводов, приклеивания к ним сторонних предметов и устройств.

При производстве отдельных следственных действий для обнаружения и фиксации следов совершения преступления, а также иной компьютерной информации, имеющей значение для дела и находящихся в памяти ЭВМ, системы ЭВМ или их сети, могут быть применены специальные программно-технические средства.

Следователь принимает решение о применении специальных программно-технических средств до начала следственного действия и уведомляет об этом всех лиц, участвующих в проведении данного следственного действия.

В случае использования при проведении отдельных следственных действий специальных программно-технических средств в протоколе следственного действия должны быть указаны объекты, к которым они были применены, а также сведения отражающие:

- наименование, версию и основные цели использования специальных программно-технических средств;
- установленные действующими федеральными стандартами параметры цифровой подписи для используемого программно-технического средства;
- порядок их начальной установки (использования) или приведения в работоспособное состояние;
- порядок и условия их подключения, запуска или приведения в работоспособное состояние для выполнения своего функционального назначения;
- порядок и условия выдачи результатов применения специальных технических и программных средств.

Рост количества совершаемых компьютерных преступлений, их высокая латентность, а также резкое увеличение размера наносимого ими ущерба, ставят разработку методики расследования данного вида преступлений в ряд первоочередных задач борьбы с преступностью.

Одной из важнейших задач в рамках создания методики расследования компьютерных преступлений является исследование проблемы образования, фиксации, а главное, выявление следов преступления. В силу специфики их образования затруднительным представляется определение природы этих следов, в частности, некоторые авторы (А.В. Мещеряков) выделяют такое понятие, как "виртуальные следы" преступления (как промежуточные между материальными и идеальными), которые отражают особенность такого материального носителя следов как электромагнитное поле.

Приведенная точка зрения может расцениваться как неоднозначная и спорная, но, тем не менее, она лишний раз подчеркивает необходимость наличия специальных знаний у сотрудников органов дознания и предварительного следствия в области информационных технологий и виртуального программного обеспечения.

Хочется надеяться на то, что работники правоохранительных органов будут чаще и теснее сотрудничать со специалистами данной сферы. Повышение уровня знаний в нашем современном обществе является непосредственной необходимостью. И все идет к тому, что в ближайшем будущем процент компьютерных преступлений по отношению ко всем преступлениям достигнет достаточно высокой планки.