С. А. Ковалев

К ВОПРОСУ О СЛЕДООБРАЗОВАНИИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья посвящена актуальным вопросам выявления следов преступного деяния при расследовании преступлений в сфере компьютерной информации. В ней рассмотрены классификация следов, природа их возникновения и способы их выявления.

Ключевые слова: информация, компьютерная информация, следы, следообразование, преступление, расследование.

S. A. Kovalev

TO THE QUESTION OF TRACES APPEARANCE IN CRIMINAL INVESTIGATION IN THE SPHERE OF COMPUTER INFORMATION

In the article urgent questions of detection of crime traces in case of investigation in the sphere of computer information are analyzed. There is also a classification of traces. Character of their appearance and methods of their detection are described.

Keywords: information, computer information, traces, crime, origin of traces, investigation.

Общеизвестно, что при совершении какого-либо преступного деяния на месте совершения преступления остаются различные следы преступной деятельности, исключением не являются и преступления, совершаемые в сфере компьютерной информации (под следами преступления понимают любые изменения среды, возникшие в результате совершения в этой среде преступления).

Следы совершения преступления в сфере компьютерной информации в силу специфики рассматриваемого вида преступлений редко остаются в виде изменений внешней среды. Они в основном не рассматриваются современной трасологией, поскольку в большинстве случаев носят информационный характер, т. е. представляют собой те или иные изменения в компьютерной информации, имеющие форму ее уничтожения, модификации, копирования, блокирования. Как справедливо отмечает А. В. Касаткин, «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, с. 14].

По делам о преступлениях в сфере компьютерной информации целесообразно следы преступной деятельности разделить на два типа: традиционные следы (следы-отображения, рассматриваемые трасологией, 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. Материальные следы могут остаться и на самой вычислительной технике (следы пальцев рук, микрочастицы на мониторе, клавиатуре, мышке, дисководах, принтере и т. д.), а также на магнитных и оптических носителях информации.

В свою очередь, информационные следы

образуются в результате воздействия (уничтожения, модификации, копирования, блокирования и т. д.) 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 (по сравнению с исходным состоянием). Речь идет о следах модификации информации (баз данных, программ, текстовых файлов), находящейся на жестких дисках ЭВМ, дискетах, магнитных лентах, лазерных и магнито-опти-ческих дисках. Кроме того, магнитные носители могут нести следы уничтожения или модификации информации (удаление из каталогов имен файлов, стирание или добавление отдельных записей, физическое разрушение или размагничивание носителей). Информационными следами являются также результаты работы антивирусных и тестовых программ. Данные следы могут быть выявлены при изучении компьютерного оборудования, рабочих записей программистов, протоколов работы антивирусных программ, программного обеспечения. Для выявления подобных следов необходимо участие специалистов.

Информационные следы могут оставаться и при опосредованном (удаленном) доступе через компьютерные сети, например через Интернет. Они возникают в силу того, что система, через которую производится доступ, обладает некоторой информацией, которую эта система запрашивает у лица, пытающегося соединиться с другим компьютером. Она определяет электронный адрес, используемое программное обеспечение и его версию. Кроме того, при доступе в сеть обычно запрашивается логин и пароль для контроля обращений на сервер, также это позволяет провайдеру идентифицировать личность проникающего в сеть.

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, файлов и пр.

Перечисленное может свидетельствовать об изменениях в заданной структуре файловой системы, а также об изменении содержимого файлов. Кроме того, при неправомерном доступе к компьютерной информации могут быть обнаружены изменения в заданной ранее конфигурации компьютера, в том числе: изменение «обоев» рабочего стола и цвета экрана при включении; изменение порядка взаимодействия с периферийным оборудованием (принтером, модемом и др.); появление новых и удаление прежних сетевых устройств.

На неправомерный доступ к компьютерной информации могут указывать и необычные проявления в работе ЭВМ: замедленная или неправильная загрузка операционной системы; замедленная реакция ЭВМ на ввод с клавиатуры; замедленная работа с дисковыми накопителями при записи и считывании информации; неадекватная реакция машины на команды пользователя; появление на экране нестандартных символов, знаков и пр. Представляется, что данное классификационное построение согласуется с классификацией следов, описанной выше, и дополняет ее.

Одним из наиболее часто встречающихся в настоящее время видов преступлений в сфере компьютерной информации является распространение вредоносных программ типа «Троянский конь» в целях несанкционированного получения информации и паролей с компьютеров пользователей. Данные действия квалифицируются по двум статьям УК РФ (ст. 272 «Неправомерный доступ к компьютерной информации» и ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»).

В. А. Мещеряковым на примере данного вида преступлений рассмотрены особенности

механизма образования «виртуальных» следов [3].

Прежде всего необходимо отметить, что сущность и опасность вредоносных программ типа «Троянский конь» заключается в том, что они скрытно, путем обмана (под видом какой-либо полезной прикладной программы или особо популярной компьютерной игры) доставляются на компьютер-«жертву» (например, в качестве прикрепленного к посланию электронной почты исполняемого файла) и запускаются на нем. После запуска эти программы могут выполнить какую-либо примитивную отвлекающую функцию (обещанную в сопроводительном послании) или просто выдать сообщение о невозможности выполнения полезной функции. Кроме того, они записывают тело вредоносной программы в заранее установленное место на компьютере-«жертве» (главная цель данного вида вредоносных программ), прописывают условия ее активизации в системный реестр, обеспечивая тем самым запуск программы при каждом включении компьютера. Запущенная вредоносная программа устанавливает соединение с провайдером сети Интернет и настраивает определенный номер порта ввода/вывода компьютера-«жертвы» в режим, при котором к нему можно скрытно подключиться удаленному компьютеру. Вторая (сопряженная) часть такой вредоносной программы, установленная на компьютере преступника, последовательно опрашивает (посылает фиксированную последовательность данных) заданный диапазон IP-адресов на возможность удаленного подключения к фиксированному порту ввода/вывода. Наткнувшись на подготовленный первой частью вредоносной программы компьютер-«жертву», компьютер преступника устанавливает скрытный канал информационного обмена и получает возможность полного управления компьютером-«жертвой»: копирование с него текущего образа экрана монитора (так называемого скриншота) любой размещенной на нем программы, создание каталога или копирование любого файла на удаленный компьютер-жертву, запуск на нем любой программы и т. п.

Исходя из вышесказанного можно заключить, что при расследовании преступлений, совершаемых в сфере компьютерной информации, важным этапом является поиск и правильная фиксация следов. Особо следует отметить, что информационным (виртуальным) следам в силу специфики рассматриваемого вида преступлений необходимо уделять большее внимание, чем материальным.

Список библиографических ссылок

1. Белкин Р. С. Курс криминалистики: в 3 т. М., 1997. Т. 2.

2. Касаткин А. В. Тактика собирания и использования компьютерной информации при расследовании преступлений: автореф. дис. ... канд. юрид. наук. М., 1997.

3. Мещеряков В. А. Механизм следообразования при совершении преступлений в сфере компьютерной информации // Известия Тульского государственного университета. Тула, 2000. Вып. 3. С. 170—172.