В.А. Милашев

ВОПРОСЫ СЛЕДООБРАЗОВАНИЯ ПРИ УДАЛЕННОМ ВОЗДЕЙСТВИИ НА КОМПЬЮТЕРНУЮ ИНФОРМАЦИЮ В СЕТЯХ ЭВМ

Трасология исходит из того, что в материальных следах определенной группы объектов содержатся признаки, несущие информацию о внешнем строении этих объектов, индивидуально неповторимом качестве их внешнего своеобразия. Внешнее строение таких объектов определяется их пространственными границами, формой, рельефом, микрорельефом и взаимным расположением образующих элементов.

Развитие криминалистики привело к выделению из трасологии ряда следов в самостоятельные разделы. Например, следы, возникающие при применении огнестрельного оружия, стали изучаться в судебной баллистике, следы подделок и подлогов в документах - в разделе технико-криминалистического исследования документов.

Сегодня в связи с всесторонним внедрением в повседневную жизнь компьютеров и количественным ростом противоправных действий, посягающих на отношения в сфере компьютерной информации, можно говорить о появлении вполне самостоятельной группы следов противоправного воздействия на ЭВМ и их сети. Изучение этих следов и механизма их образования в будущем вполне может привести к формированию нового раздела в рамках криминалистической техники. Чем обусловлено такое предположение?

Следы, оставляемые при удаленном воздействии на компьютерную информацию, действительно существенно отличаются от всего, что когда либо изучалось криминалистикой.

В чем их особенность? Единицей компьютерной информации является бит, имеющий два значения – "0" или "1". Совокупность битов образует байты, из которых складываются двоичные данные. Система их взаимодействия подчинена законам логики и математики. Отсюда следует, что закономерности иных наук (физики, механики и т.д.) не могут быть использованы для объяснения механизма образования следов противоправной деятельности. Механизм взаимодействия двух различных двоичных кодов не позволяет применять к ним такие концептуальные для криминалистики понятия, как следообразующий объект, следовоспринимающий объект и следовой контакт, в том узком содержательном аспекте, который придает им криминалистика, ввиду отсутствия внешнего строения у компьютерной информации. Действительно, взаимодействие компьютерной информации, воздействующей на ЭВМ, и той, которая содержится в ЭВМ жертвы, происходит не на уровне физического отражения внешнего строения, а на

уровне логической организации работы компьютера. Объяснить характер изменений в компьютере, произошедших под воздействием компьютерной информации, направленной злоумышленником, можно только через призму организации работы компьютера в целом и отдельных программ.

Учитывая, что следами противоправной деятельности являются результаты логических и математических операций с двоичным кодом, мы предлагаем называть их *бинарными следами*.

Принимая во внимание интенсивное применение сетевых компьютерных технологий в различные сферах жизни, очевидно, в будущем придется сталкиваться в основном с бинарными следами, образующимися при *удаленном воздействии* на ЭВМ и их сети - новом способе совершения преступления, при котором злоумышленник применяет приемы и средства, основанные на использовании механизма взаимодействия ЭВМ в сетях.

Несмотря на своеобразие этих следов, все же они носят материальный характер, что позволяет к ним относится просто как к новым, ране неизвестным криминалистике, объектам. А это вселяет убеждение, что бинарные следы будут изучены.

Следовая картина является важным элементом механизма преступной деятельности. Она включает в себя: локализацию (место отображения следовых картин), форму отображения (вещественная, документальная, идеальная), релевантность (относимость к событию преступления), информативность (количественная и качественная характеристики следовых картин) [1].

Так как компьютер способен обрабатывать только двоичный код, то и само удаленное воздействие представляет собой совокупность управляющих данных в двоичной форме, направленных в адрес удаленного компьютера по сети связи. При этом и формирование сигнала в компьютере злоумышленника, и обработка его промежуточными компьютерами, и обработка его в компьютере жертвы ведут к изменению двоичного кода и образованию бинарных следов в каждом из перечисленных компьютеров.

Так как выявление бинарных следов возможно только при их считывании в энергозависимую память и преобразовании до уровня архитектуры компьютера, позволяющего их наблюдать на устройствах вывода в доступной для восприятия форме, требует уточнения вопрос о том, как такие следы проявляются:

- в компьютере злоумышленника;
- в промежуточном компьютере;
- в компьютере жертвы.

Для выявления областей локализации следов, по мнению автора, целесообразно упорядочить сведения о видах компьютерной информации, с

помощью которой злоумышленник воздействует на удаленный компьютер.

Бинарный след является итогом взаимодействия двоичных кодов. В зависимости от того, какую роль в компьютере они выполняют, различными будут и бинарные следы.

Весь спектр возможных воздействий на компьютер можно условно разделить на 3 группы:

- команды процессам;
- запуск процессов;
- воздействие коммуникационными сигналами сетевых протоколов.

Литература

1. Лубин А.Ф. Механизм преступной деятельности. Методология криминалистического исследования. -Н. Новгород, 1997. -143 с.