ОСОБЕННОСТИ СЛЕДОВОЙ КАРТИНЫ ПО КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

Е.Е. Сторожева
Алтайский государственный университет, г. Барнаул

На сегодняшний день проблема следовой картины по компьютерным преступлениям является наиболее актуальной в связи с тем, что данные следы не имеют определённых характеристик, характеристики которые должны здесь применяться являются специфическими и в криминалистике не разработаны.

В юридической литературе рассматривается определение следа в широком и узком смысле. След в широком смысле представляет собой любое изменение в материальной среде, возникающее в ней в результате, совершённого преступления. След в узком смысле представляет собой отображение на одном из взаимодействовавших в процессе совершения преступления объектов, внешнего строения другого объекта. Выделяется два основных вида следов: материальные и идеальные. Материальные следы преступления являются основой учения о следах (трасологии) и включают в себя: следы-отображения, следы-предметы, следы-вещества. Идеальные следы преступления представляют собой некое отображение события в памяти человека, знания о свойствах данных событий, которые заимствуются из различных научных познаний.

По современным представлениям фиксация следов в памяти осуществляется в три этапа: сначала в иконической (сенсорной) памяти на основе деятельности анализаторов; затем информация, полученная посредством анализаторов, направляется в высшие отделы головного мозга, где происходит анализ, сортировка и переработка сигналов; на третьем этапе информация переводится в долговременную память[1]. В данной связи, как и с мозгом человека, который принимает информацию и пропускает её через определённые этапы, мы можем говорить и об информации, которая поступает на соответствующий компьютер. Мы можем выявить центр (компьютер, смартфон и т.д.), где происходило преступление, зафиксировать импульс который идёт по кабелю в момент передачи информации, а также намагниченность соответствующей ветви.

В силу существования двух основных видов следов, возникает вопрос, следы, оставшиеся в результате совершения компьютерных преступлений, являются материальными или идеальными? А может они являются ещё одной разновидностью следов?

В данной связи, ряд авторов, такие как: В.А. Мещеряков, А.Г. Волеводз, В.Е. Козлов, В.В. Поляков, А. Семенов, выделяют данные следы как ещё один вид следов в криминалистике и именуют их «виртуальными». Выделяя их в новый вид, представители данной точки зрения делятся на две группы: те, которые отмечают пограничное место виртуальных следов между материальными и идеальными и те, кто рассматривает их как одну из разновидностей материальных следов. Выделяя данные следы как самостоятельный вид следов в криминалистике, авторы предлагают их различные названия. А.Г. Волеводзпредлагает обозначить данные следы как виртуальные, под которыми в свою очередь понимаются: «виртуальные следы» - это данные о происхождении информации: таблицы размещения файлов (FAT, NTFS или другие), системные реестры операционных систем, отдельные кластеры магнитного носителя информации, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удалённого доступа и иное [2]. В.Е. Козлов поддерживает позицию А.Г. Волеводза, однако трактует данное определение немного иначе: «виртуальный след» - это система команд ЭВМ, где виртуальный объект будет являться следообразующим [3]. В.А. Милашев предлагает обозначить данные следы бинарными, под которыми понимаются: «бинарные следы» - это следы, как результат логических и математических операций с двоичным кодом [4]. Д.А. Турчин обозначает данные следы компьютерно-техническими, под которыми следует понимать: «компьютерно-технические следы» - это следы, отражающие особую – информационную среду и представляющие собой электронный код и сигнал, передаваемый на уровне пользователей, предполагая наличие источника, носителя, владельца (потребителя) и среды [5].

На основании вышеизложенного считаем, что на сегодняшний день, данный вопрос до сих пор является дискуссионным. Полагаем более удачной позицию авторов, именующих данные следы «виртуальными». А.Л. Осипенко указывает на особую сложность обнаружения следов, обуславливая этот факт особенностями сети Интернет. Подчёркивая, что следы преступных действий будут распределены по множеству объектов (компьютерная система жертвы, преступника, провайдера, промежуточные сетевые узлы и т.п.) [6].

В данной связи возникает ещё один вопрос - как обнаружить данную категорию следов. В ряде научных работ, говорится о том, что один из основных способов сокрытия компьютерных

преступлений – инсценировка. Р.С. Белкин определяет инсценировку, как – создание обстановки, не соответствующей фактически происшедшему на этом месте событию, что может дополняться согласуемыми с этой обстановкой поведением и ложными сообщениями как исполнителей инсценировки, так и связанных с ними лиц[7].Сущностную сторону инсценировки более точно выразил П.В. Малышкин: «Преступную инсценировку можно определить как обстановку мнимого события, созданную искусственным путём и образовавшуюся в результате деятельность субъекта, которая может дополняться соответственным его притворным поведением, согласуемым с данной обстановкой, и произведённую с целью сокрытия преступления и уклонения от ответственности за содеянное» [8].Особенность проявления инсценировки по компьютерным преступлениям заключается в том, что преступник предпринимает попытки создать некую виртуальную реальность, которая искажает действительно имевшие место быть события, факты. Инсценировка производится с помощью специальных программ, которые при совершении преступления, становятся средством его совершения. Именно благодаря тому средству, который использовал преступник при совершении преступления, мы можем выявить вид и способ инсценировки. В данном связи, можем сделать вывод о том, что инсценировка представляет собой некое создание видимости существования определённого факта, которого на самом деле не было, и который подменяет тот факт, который на самом деле имел место. Необходимо отметить, что при инсценировке работа следователя по обнаружению данных следов заметно усложняется. Сложность заключается в том, что данные следы очень сложно выявить, а так же в том, что нет определённых рекомендаций, форм изъятия данных следов. Вышеперечисленное, позволяет сделать вывод, что сложность в выявлении и изъятии следов по компьютерным преступлениям может служить основанием фальсификации данных следов, их удаления, а также внесения недостоверных данных третьими лицами.

Однако необходимо отметить, что выявление и фиксация следов по компьютерным преступлениям возможны с помощью судебной компьютерно-технической экспертизы. Необходимость в судебной компьтерно-технической экспертизе обуславливается широким внедрением компьютерных технологий практически во все сферы человеческой деятельности. Данные экспертизы проводятся в целях определения статуса объекта как компьютерного средства,

выявления и изучения его роли в совершённом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним её исследованием. Проведение компьютерно-технической экспертизы позволяет установить возможность осуществления доступа с помощью представленного на исследование объекта к локальной или глобальной сети, выявить информационные следы преступления, определить вид последствий неправомерного доступа к компьютерной информации либо установить причастность лица к совершению преступления, либо определить механизм совершения неправомерного доступа[9].Помимо проведения судебной компьютерно-тезхнической экспертизы, часто приходится прибегать к назначению почерковедческой экспертизы. Данная экспертиза назначается в том случае, если при проведении следственных мероприятий на месте совершения преступления были найдены блокноты, записки, чертежи и т.д. и содержание которых может явиться одним из доказательств совершения преступления конкретным лицом. Результаты проведения экспертиз, зачастую позволяют определить причастность того или иного лица к совершению конкретного преступления, а также установить механизм совершения преступления, а при инсценировке – его способ.

Таким образом, нужно отметить, что вопрос о понятии следов, оставленных в результате совершения компьютерных преступлений, является дискуссионным. Полагаем, что целесообразно именовать их как «виртуальные» следы. Вопрос об обнаружении данных следов усложняется в связи с появлением такой формы противодействия расследованию преступлений в сфере компьютерной информации, как инсценировка. Благодаря ей возможна фальсификация и удаление важной для следствия информации, а также следов совершения преступления.

Библиографический список

1. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – Взамен ГОСТ Р ИСО/МЭК 15408-1-2008; Введ. 01 – 12 – 2013. – Москва: Стандартинформ, 2014.

2. Мочагин П.В. Виртуально – информационный и невербальный процесс отражения следообразований как новое направление в криминалистике и судебной экспертизе // Вестник Удмуртского университета. – 2013. –Вып. 2. – С. 148-154.

3. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. – 2002. - №1. – С. 4.
4. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия – Телеком, 2002. – С. 336.
5. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: автореф.дисс. – М.: МГУ им. М.Ю. Ломоносова, 2004. – С. 18.
6. Турчин Д.А. Теоретические основы трасологической идентификации в криминалистике. Владивосток: Изд-во Дальневосточного ун-ва, 1983. – С. 187.
7. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская акад. МВД России, 2009. – С. 480.
8. Белкин Р.С. Курс криминалистики: в 3т. М., 1997. Т.3. – С. 372.
9. Малышкин П.В. Распознание преступных инсценировок при криминалистическом исследовании обстановки места происшествия: дисс. – М., 1990. – С. 41.
10. Егорышева Е.А., Егорышев А.С. Некоторые вопросы использования специальных знаний при расследовании неправомерного доступа к компьютерной информации // Эксперт-криминалист. – 2011. - №3. – С. 14-15.