Ершова А.Н.
Научный руководитель - Е.А. Ануфриева, к.ю.н., преп.

ЗНАЧЕНИЕ ЭЛЕКТРОННО-ЦИФРОВЫХ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

С конца 90-х годов в России происходит стремительное развитие и распространение информационных технологий. Радикальные изменения в информационных отношениях общества связаны, прежде всего, с применением глобальных компьютерных сетей, в первую очередь информационной сети Интернет. Процесс информатизации общества сопровождался быстрым ростом компьютерной грамотности, особенно среди молодежи. Доступными стали средства компьютерной техники и практически любое программное обеспечение, в том числе вредоносное. Все эти обстоятельства привели к резкому обострению криминальной обстановки в информационной сфере общества [1].

Криминализация информационной сферы нашла свое отражение в появлении новых видов и форм преступлений, связанных с применением последних достижений науки и техники, такие преступления являются сложными и высокотехнологичными. Эти преступления характеризует исключительно высокий уровень латентности в сочетании с низким уровнем раскрываемости. Так, в 2011 году в нашей стране совершено 2698 компьютерных преступлений [2].

Существенное значение при расследовании неправомерного доступа к компьютерной информации имеет исследование механизма следообразования, представляющего собой наиболее стабильный и наиболее значимый элемент криминалистической характеристики преступлений [1]. Зная тонкости процесса образования следов неправомерного доступа к компьютерной информации можно легко судить о способе совершения преступления, действиях по сокрытию данного преступления, некоторых особенностях лица, совершившего преступление, а также об обстановке совершения данного преступления. Выявление, фиксация и изъятие следов неправомерного доступа к компьютерной информации играет определяющую роль в сборе доказательственной базы при расследовании данных преступлений. На основе информации, получаемой при изучении следов, могут быть построены версии об участниках преступления. Во многом следовая картина определяет тактику расследования преступления.

В соответствии с общепринятыми положениями криминалистического учения все следы совершения любого преступления делятся на две основные группы: материальные, т.е. зафиксированные в виде изменения внешней среды и объектов, ее образующих; идеальные, т.е. оставшиеся в памяти преступника, соучастников и свидетелей [2]. Вместе с тем, в механизме следообразования при неправомерном доступе к компьютерной информации можно выделить особую специфическую группу следов, нехарактерную для большинства других

видов преступлений. Речь идет о следах, оставленных в информационном пространстве компьютерных иных цифровых устройств, их систем и сетей при совершении неправомерного доступа к компьютерной информации путем ее уничтожения, блокирования, модификации либо копирования. Изучение следов данного вида началось в криминалистике не так давно и на сегодняшний день в криминалистической литературе нет однозначного мнения о том, каким термином следует обозначать такие следы, а также о том, каким образом их следует включить в существующую в криминалистике классификацию следов преступления.

Авторами предлагаются самые разнообразные термины для обозначения данной группы следов: виртуальные [5, информационные [6], электронно-цифровые [7], бинарные [8], компьютеро-технические [9] и другие.

Из всего многообразия высказанных предложений, по нашему мнению, наиболее точным термином для рассматриваемой группы следов является «электронно-цифровые следы», поскольку в результате электронно-цифрового отражения на материальном носителе фиксируется цифровой образ, состоящий из цифровых значений параметров формальной математической модели наблюдаемого реального физического явления [10].

Говоря о месте электронно-цифровых следов в системе криминалистической классификации следов преступления, следует отметить, что учеными высказываются две точки зрения. Согласно первой электронно-цифровые следы следует выделить в качестве третьей группы следов [11]. Так, В.А. Мещеряков отмечает, что основными взаимодействующими объектами при совершении данного вида преступлений являются информационные объекты, обладающие сложной иерархической структурой, при рассмотрении которой говорить о внешнем строении (т.е. какой-либо материальной форме проявления) или его особенностях не приходится [12]. Однако представленная позиция, по нашему мнению, далеко не лишена дискуссионности, Нами разделяется точка зрения другой группы криминалистов, которые полагают, что электронно-цифровые следы следует отнести к группе материальных следов, поскольку данные следы являются материальными невидимыми следами, так как они зафиксированы на материальном носителе либо передаются по каналам связи посредством электромагнитных сигналов.

Немаловажным в теоретическом плане является вопрос о классификации электронно-цифровых следов. Предложим несколько вариантов таких классификаций по различным основаниям. Так, А.Ю. Семенов, одним из оснований для классификации выделяет непосредственный физический носитель «виртуального следа». На таком основании можно выделить:

1. следы на жестком диске (винчестере), магнитной ленте («стримере»), оптическом диске (CD, DVD), на дискете (флоппи диске);
2. следы в оперативных запоминающих устройствах (ОЗУ) ЭВМ;
3. следы в ОЗУ периферийных устройств (лазерного принтера, например);
4. следы в ОЗУ компьютерных устройств связи и сетевых устройств;
5. следы в проводных, радио-оптических и других электромагнитных систем и сетей связи.

Представляется возможным классифицировать электронно-цифровые следы по месту их нахождения на 2 группы:

1. следы на компьютере преступника;

2. следы на «компьютере-жертве» [13].

По мнению В.Ю. Агибалова создание какой-либо статической системы классификации электронно-цифровых следов является бесперспективным вследствие высокой динамичности развития технических средств; наиболее оправданным направлением классификационных исследований будет использование фасетного метода, который позволит:

- постоянно совершенствовать созданные классификации без их коренной структурной переделки;

- систематизировать и хранить сведения об используемых приемах преобразования информации и порождаемых ими особенностях виртуальных следов;

- кодировать и индексировать используемые преобразования цифровой информации на каждом из этапов формирования виртуального следа для обеспечения возможности сопоставления с каждым из них необходимого комплекса программно-аппаратных средств, позволяющих выявлять и извлекать виртуальные следы;

- формировать перечни типовых сценариев применения программно-аппаратных средств выявления и извлечения виртуальных следов, что в свою очередь послужит основой автоматизации предварительного исследования цифровых объектов, с которыми приходится сталкиваться следователю [14].

На наш взгляд, виды электронно-цифровых следов в научной литературе достаточно четко не разработаны. Исследование данной проблемы находится только в стадии разработки, выдвигаются отдельные мнения по поводу классификации таких следов, однако определенной классификации таких следов учеными пока не предложено.

В процессе расследования таких преступлений нередко возникают трудности, которые не всегда успешно преодолеваются следователями. Анализ следственной практики показывает, что по-прежнему сильна разобщенность в действиях по своевременному обмену и проверке информации о лицах и фактах, представляющих оперативный и следственный интерес; не в полную меру используются возможности экспертно-криминалистических подразделений и помощь специалистов для обнаружения, фиксации, исследования и изъятия специфических вещественных доказательств; медленно решаются вопросы информационного обеспечения выявления, раскрытия и расследования преступлений в сфере компьютерной информации; существуют серьезные проблемы с подготовкой и переподготовкой квалифицированных специалистов по этой линии работы. Необычность рассмотрения следов неправомерного доступа ккомпьютерной информации приводит к тому, что большинство следователей не готовы к их выявлению и закреплению в соответствии с действующим законодательством.

Ввиду отсутствия достаточного числа специалистов в сфере информатики в правоохранительных органах, получение полезной для расследования

информации из ЭВМ на практике достаточно проблематично. Решение данной задачи становится практически невозможным, если преступники, обладая профессиональными навыками работы с ЭВМ, уничтожают виртуальные следы. На практике серьезные проблемы может вызвать обнаружение, изъятие и фиксация материально фиксированных следов. Это связано с тем, что в большинстве случаев одним персональным компьютером может пользоваться неограниченное число пользователей. Это обстоятельство является причиной того, что на различных частях компьютера можно обнаружить большое количество отпечатков пальцев, принадлежащих нескольким людям. Как показал проведенный анализ специальной криминалистической литературы и практического опыта работников правоохранительных органов, к числу таких специфических свойств, в первую очередь, следует отнести следующие:

- трудности в определении места происшествия и установлении его границ (в рамках которых должен проходить следственный осмотр), а также в реализации тактических рекомендаций по проведению следственного осмотра;
- необходимость активного использования специальных знаний при подготовке и проведении следственного осмотра;
- необходимость подготовки и использования специальных аппаратных и программных средств, позволяющих выявить, извлечь и зафиксировать виртуальные следы (уголовно-релевантную компьютерную информацию). Ввиду отсутствия специализированных криминалистических средств выявления и изъятия следов неправомерного доступа к компьютерной информации в повседневной деятельности правоохранительных органов используется достаточно широкий набор стандартных программных средств общего применения, которые условно можно разделить на два основных класса: универсальные (многоцелевые) и специализированные (выполняющие определенный круг задач) программные средства.

Наличие недостатков в сфере поиска, обнаружения и изъятия следов неправомерного доступа к компьютерной информации, а также тот факт, что большинство из них являются зарубежными разработками, для которых отсутствуют исходные коды программ (что не позволяет с большой степенью уверенности судить о всех их функциях и возможностях), приводит к выводу о необходимости создания отечественного специализированного программного средства, которое могло бы использоваться в своей деятельности правоохранительными органами.

Большинство крупных компаний ведут специальные электронные протоколы (журналы, лог-файлы), в которых протоколируются данные о запросах их информационных ресурсов и о происходящем информационном обмене [15].LOG-файлы (и соответственно сохраняемые ими сведения о сообщениях, передаваемых по сетям электросвязи) следует признать наиболее значимыми носителями следовой информации о совершении преступлений в компьютерных сетях.

В силу этого логичным явилось бы их сохранение поставщиками услуг (провайдерами) в своеобразных электронных архивах. Соглашаясь с позицией А.Г. Волеводза, мы считаем необходимым на законодательном уровне

установить единые стандарты сохранения сведений о сообщениях, передаваемых по сетям электросвязи, разработать единые требования к объему и номенклатуре подлежащей обязательному сохранению компьютерной информации, определить оптимальные сроки такого сохранения, установить особый порядок ее документирования при необходимости передачи компетентным органам, разработать правила и порядок уничтожения [16].

Для решения данных проблем на наш взгляд необходимо:

- создание специализированных следственных подразделений, укомплектованных специалистами, владеющими всеми необходимыми знаниями и навыками для поиска и обращения со следами;
- законодательное закрепление обязанности участия специалиста в проведении следственных действий, связанных с обнаружением и фиксацией следов. При этом желательно участие одного и того же специалиста во всех соответствующих следственных действиях одного уголовного дела, так как это позволит ему более качественно выполнить свои обязанности, а следователю - полнее применить его специальные навыки и познания для уяснения общей картины преступления, а не только отдельных эпизодов или фактов (явлений);
- следователям проходить специальную подготовку по изучению специфики расследования неправомерного доступа к компьютерной информации, выявления и фиксации следов неправомерного доступа к компьютерной информации, принципов работы ЭВМ;
- создание специализированных криминалистических справочников;

Для надежной фиксации и сохранения всестороннего, полного и объективного изучения всех следов, имеющихся на компьютере, необходимо предпринимать следующие меры:

- на месте постоянного нахождения компьютера не разрешать, кому бы то ни было из лиц, находящихся, работающих в помещении, где находится ЭВМ и периферийные устройства, прикасаться к ним с любой целью;
- никому из персонала и прочим лицам не разрешать выключать электроснабжение объекта осмотра или выключать ЭВМ из сети;
- самостоятельно не производить никаких манипуляций с ЭВМ и периферийными устройствами, не будучи абсолютно уверенным в последствии своих манипуляций;
- перед выключением питания ЭВМ закрыть подобающим способом все программы и приложения;
- принять меры по установлению паролей и кодов доступа к защищенным программам;
- при нахождении ЭВМ в локальной сети при осмотре необходимо присутствие специалистов, которые смогут быстро прореагировать на перемещение информации в сети;
- произвести осмотр всей документации, записок, различных бумаг, которые находятся в непосредственной близости от компьютера или принадлежат человеку, который работает с ним.

Выполнение этих условий поможет сохранить на ЭВМ и периферийных устройствах информацию, которая может оказаться полезной при дальнейшем

подробном исследовании данных объектов. Таким образом, получить наиболее объективную информацию о следах, имеющихся на компьютере и сопутствующих объектах. Кроме этого, необходимо внедрять все новые средства и методики изучения рассматриваемой группы следов в практическую деятельность работников правоохранительных органов.

Библиографический список

1. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф-т дисс. ... канд. юрид. наук. - Омск, 2008.- С. 2.
2. Костомаров К.В. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков : автореф-т дисс. ... канд. юрид. наук.. - Челябинск, 2012. - С. 2.
3. Баев О.Я. Методические основы расследования преступлений против личности // Расследование преступлений против личности. - Воронеж, 1998. - С. 11.
4. Яблоков Н.П. Криминалистика М.: Юристь, 2005. С. 53.
5. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования: моногр. Воронеж, 2002 г. С. 102.
6. Шурухнов Н.Г.Расследование неправомерного доступа к компьютерной информации
7. Ищенко Е.П., Топорков А.А. Криминалистика 2009г. С. 29; Вехов В.Б. Понятие, особенности механизма образования, криминалистические классификации электронно-цифровых, оптических и магнитных следов.
8. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: Автореф. дис. ... канд. юрид. наук. М., 2004. С. 18.
9. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: Автореф. дис. ... канд. юрид. наук. М., 2007. С. 11.
10. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: Автореф. дис. ... канд. юрид. наук. Воронеж: ГОУ ВПО "Воронежский государственный университет", 2010. С. 13.
11. Шурухнов Н.Г. Расследование неправомерного доступа к компьютерной информации, Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования: моногр. Воронеж, 2002 г. С. 94.
12. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования: моногр. Воронеж, 2002 г. С. 96.
13. Семенов А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации / Сибирский Юридический Вестник. - 2004. - №
14. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе Воронеж - 2010. С. 14-15

15. Собецкий И.В. О доказательственном значении лог-файлов. http://'www.securitylab.ru/39167.html
16. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях С - 5