УДК 343.985

Н.Н. Беломытцев, *адъюнкт научно-педагогического факультета*
Академии МВД Республики Беларусь
(e-mail: belomitcev64@gmail.com)

ОСОБЕННОСТИ ОБРАЗОВАНИЯ СЛЕДОВ ПРИ СОВЕРШЕНИИ ХИЩЕНИЯ ПУТЕМ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ

В двух частях

Часть 1

Анализируется механизм образования, а также рассматриваются существующие классификации следов совершения хищения путем использования компьютерной техники. Исследуются актуальные теоретические и прикладные вопросы, связанные с определением понятия электронно-цифровых следов, изучение которых обосновывает использование категории «электронно-цифровой след».

Ключевые слова: электронно-цифровой след, механизм следообразования, носитель электронно-цифровой информации.

Расследование любого вида преступного деяния в первую очередь связано со сбором информации, имеющей отношение к произошедшему событию. Преступления, в которых средством их совершения выступают компьютерные и иные программно-технические средства, имеют специфическую следовую картину. Остаются следы также на всевозможных носителях цифровой информации. Сбор непосредственно материальных или идеальных следов в традиционном их понимании у большинства сотрудников обычно не вызывает особых затруднений, однако при работе с электронно-цифровыми следами появляются определенные сложности. В этой связи специфика механизма электронно-цифрового следообразования при совершении хищений путем использования компьютерной техники требует более глубокого осмысления и исследования.

В мировой практике изучением понятия следов, процесса их образования, установления, выявления, фиксации и сбора занимались Б.И. Шевченко, Л.К. Литвиненко, Д.А. Турчин, И.Н. Якимов, И.Ф. Крылов, Г.Л. Грановский; экспертным исследованием следов – С.М. Потапов, А.Н. Василевский и И.М. Зельдес. Непосредственно вопросы классификации следов рассматривались в специальных исследованиях, среди которых необходимо отметить публикации А.Р. Белкина, Б.М. Комаринца, Г.Л. Грановского, Г.А. Матусовского, В.Е. Корноухова, И.Н. Пророкова, В.А. Образцова, Д.И. Шевченко, В.И. Попова, И.Н. Якимова и др.

Анализ современных теоретических, практических и научных исследований показал, что деление следов преступлений на материальные (зафиксированные в виде изменения внешней среды и объектов, ее образующих (следы-отображения, следы-вещества, следы-предметы)) и идеальные (оставшиеся в памяти подозреваемых (обвиняемых), потерпевших и свидетелей) обусловливает свою эффективность и значимость при расследовании практически всех видов преступлений, в том числе и против информационной безопасности, к которым, на наш взгляд, в определенной степени относятся и хищения путем использования компьютерной техники. При этом мы исходим из того, что теоретические основы материальных и идеальных следов достаточно всесторонне и полно разработаны в криминалистической науке и соответственно не нуждаются в дополнительных пояснениях.

Теория отображения гласит, что любая подготовка обладает свойством отражения – способностью материальных объектов при взаимодействии между собой запечатлевать воздействия на них других материальных объектов. С позиции указанной теории подготовка, совершение и сокрытие любого преступления, в том числе хищения путем использования компьютерной техники, как определенное событие материального мира всегда влечет за собой определенные изменения в окружающей среде, так как отражение присутствует всегда, когда происходит взаимодействие двух и более материальных объектов. Таким образом, можно сказать, что любые преступные действия – это оставленные следы (материальные, идеальные, на носителях цифровой информации), которые сохраняются на следовоспринимающем объекте определенное время.

В рамках вопроса о процессе следообразования логично обратиться к мнению Р.С. Белкина. Ученый считает, что природа информации, носителями которой выступают объекты следообразования, различна. При этом следообразующий (отражаемый) объект – носитель непосредственной, первичной информации, выражающейся в совокупности присущих ему индивидуальных и устойчивых свойств и признаков; следовоспринимающий (отражающий) объект – носитель отраженной, производной от первого объекта, «вторичной» информации, возникшей вследствие контакта, т. е. взаимодействия. В результате взаимодействия указанных объектов, по мнению Р.С. Белкина, устанавливается причинно-следственная связь между ними на основе их связи с произошедшим событием. Но здесь важно понимать, что следовоспринимающий объект несет информацию не только об отражаемом объекте, а является носителем информации о механизме следообразования, т. е. о действиях с отражаемым объектом или самого отражаемого объекта. В данном случае отражаемый объект выступает средством передачи информации о способе, а через него – и о субъекте действия [1, с. 63]. Такая информация передается от материального объекта к другому материальному объекту, а при совершении хищений (путем использования компьютерной техники) передается в первую очередь при помощи электронно-цифровых носителей данных – следовоспринимающих объектов. Следовательно, информация может быть передана в пространстве, сохранена во времени и подвергнута обработке.

До настоящего времени электронно-цифровые (виртуальные) следы чаще всего исследовались в контексте изучения отдельных аспектов расследования преступлений против информационной безопасности, специфики следственных действий и экспертных исследований компьютерной техники. Непосредственно исследования, посвященные электронно-цифровым следам, феномену их образования, отображения как в цифровом, так и в реальном мире занимались В.А. Мещеряков [2], В.Ю. Агибалов [3], В.Б. Вехов [4], В.А. Милашев [5], П.В. Мочагин [6], А.В. Касаткин [7], Ю.В. Гаврилин [8] и др. В отношении названия данных следов, их содержания и места в теории криминалистики учеными высказывались различные мнения. Многие авторы считают необходимым выделение электронно-цифровых следов в отельную группу, называя их виртуальными (В.А. Мещеряков), «бинарными» (В.А. Милашев), виртуально-информационными (П.В. Мочагин), компьютерными (А.В. Касаткин) и т. д. Некоторые авторы также указывают на уникальность образования, существования и исследования данных следов, при этом обосновывая материальную суть и природу электронно-цифровых следов (Ю.В. Гаврилин).

Так, по мнению В.Б. Вехова, электронно-цифровой след – это любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий, либо передающиеся по каналам связи посредством электромагнитных сигналов [4, с. 90, 94]. По мнению В.Н. Черкасова, следы на компьютерных носителях по сути являются материальными и не отличаются от иных следов за исключением сложности инструмента и процесса их образования. Однако указанное не является поводом для пересмотра методологии и понятийного аппарата, а только причиной для совершенствования конкретных, реальных, практических методик и методов [9, с. 70]. Е.А. Лушин также считает данные следы электронно-цифровыми, так как в компьютерных системах они образуются в результате движения электронов и хранятся в памяти электронных устройств в виде двоичного кода [10, с. 161].

Видится логичным согласиться с мнением вышеперечисленных авторов в отношении названия «электронно-цифровые следы», так как следы от воздействия электронов могут оставаться не только на различных носителях данных, но и на других объектах (например, на перегоревшем шлейфе проводов, который нагрелся от воздействия электрического тока, т. е. в результате движения электронов в проводнике). В этой связи для конкретизации и отличия понятий целесообразно использовать и слово «цифровые», потому что в памяти электронных устройств данные представлены в виде именно цифрового кода, или изменения, образованные движением электронов и зафиксированные в цифровом (двоичном) коде.

В рамках исследуемого вопроса важно учитывать и тот факт, что в основе механизма образования рассматриваемых следов заложено особое электронно-цифровое отображение, возникающее в искусственно созданных средах: канале связи, информационной (операционной) системе, информационно-телекоммуникационной сети, памяти различных электронно-цифровых носителей информации и т. д. В этой связи качественные характеристики отображенных данных напрямую зависят от особенностей данных сред, специально заложенных разработчиками. Названные факторы определяют объем получаемых криминалистически значимых признаков и сведений, которые в дальнейшем обычно связаны с уголовно-релевантной информацией, содержащейся в формирующихся электронно-цифровых следах. При этом на электронно-цифровом носителе фиксируются не свойства наблюдаемого физического процесса (звук, изображение, видео и т. п.), а только цифровые значения параметров определенной математической модели, заложенной в основу программно-технического устройства регистрации его фактического проявления.

Зафиксированный на электронно-цифровом носителе информации след представляет собой сложную структуру данных, в которой вместе со значимой для расследования уголовного дела информацией содержится определенный объем вспомогательных данных, необходимых для его целостности и возможности расшифровки с помощью соответствующих программно-технических устройств и последующего непосредственного восприятия человеком.

В данном случае вполне обоснованным будет согласиться с мнением В.А. Мещерякова, который указывает, что электронно-цифровой след не имеет физически целостной структуры; может состоять из большого количества отдельных информационных элементов, которые при этом могут быть записаны как на одном, так и на нескольких электронно-цифровых носителях информации, подключенных к одному или нескольким (возможно, территориально расположенным на значительных расстояниях) программно-техническим средствам, объединенных в информационную систему или информационно-телекоммуникационную сеть. В данном случае получаемая структура электронно-цифрового следа в каждый конкретный момент зависит от технических особенностей регистрирующего программно-технического устройства (используемый микропроцессорный набор, вид операционной системы, вид файловой системы электронно-цифрового носителя информации, стандартов обмена информацией и т. п.) и от его текущего состояния (объем уже записанной информации на электронный носитель, включенные/выключенные параметры конфигурации аппаратного и программного обеспечения) [11, с. 269]. Соответственно, важно понимать, что электронно-цифровые данные физически не могут существовать без электронно-цифровых носителей, на которых они отображаются и хранятся.

По мнению В.Б. Вехова, электронно-цифровые носители данных относятся к категории следов-предметов или частей предметов и представляют собой технические устройства или технологические системы, предназначенные для фиксации, хранения, накопления, преобразования и (или) передачи компьютерной информации. Условно автор предлагает указанные носители разделить на семь групп:

машинные носители информации (ферромагнитная полимерная лента (полоса) или металлическая нить, гибкий полимерный или жесткий магнитный диск, жесткий оптический или магнитооптический диск и пр.);

интегральные микросхемы (идентификационные карты на интегральных микросхемах типа «sim-карта» и пр.);

микроконтроллеры (так называемые электронные проездные документы, USB-драйверы, flash-карты и пр.);

электронные вычислительные машины (компьютеры, активное серверное оборудование, банкоматы, терминалы, контрольно-кассовые машины, сотовые радиотелефоны, ресиверы, видеорегистраторы и пр.);

комбинированные носители информации (платежная карта с магнитной полосой и интегральной микросхемой и т. п.);

информационные системы;

информационно-телекоммуникационные сети (например, сеть Интернет) [12, с. 16–17].

Так, В.Е. Козлов предлагает без указания на виртуальность электронно-цифровых следов следующую их классификацию:

по характеру изменений (структурные файловые следы и внешние файловые следы);

по степени завершенности процесса обработки команд (стабильные во времени файловые следы и временные файловые следы);

по размещению (локальные файловые следы и сетевые файловые следы);

следы отображения внешнего физического воздействия на программно-технические средства (средства компьютерной техники) [13, с. 152].

А.Г. Волеводз одним из оснований для классификации рассматривает непосредственно физический носитель электронного следа и выделяет следующие следы:

на жестком диске (винчестере), магнитной ленте (стримере), оптическом диске (CD, DVD), дискете (флоппи-диске);

в оперативных запоминающих устройствах (ОЗУ) ЭВМ;

в ОЗУ периферийных устройств (например, принтера);

в ОЗУ компьютерных устройств связи и сетевых устройств;

в проводных, радио-оптических и других электромагнитных системах и сетях связи [14, с. 159].

Представленное деление, по нашему мнению, имеет определенные недостатки: количество и разновидность носителей цифровых данных постоянно увеличивается, а ранее используемые с каждым днем теряют свою актуальность или вообще перестают использоваться (магнитные ленты, дискеты и т. д.)

Любые действия с программно-техническими устройствами (смартфоны, планшеты, персональные компьютеры, ноутбуки и т. д.) получают непосредственное отражение на их носителях цифровой информации. В этой связи А.Б. Смушкин предлагает электронно-цифровые следы классифицировать по произошедшим событиям и действиям, месту их образования в памяти компьютера при эксплуатации:

включение, выключение, различные операции с содержимым памяти компьютера (отображаются в журналах администрирования, журналах безопасности и т. д.);

действия с наиболее важными для работы компьютера программами (установка, удаление и т. д.) отражаются в реестре компьютера (reg-файлах);

сведения о работе в сети Интернет, локальных и иных сетях (аккумулируются в так называемых log-файлах);

операции с файлами (отражаются в их свойствах (например, текстовые файлы с разрешением docx) время создания, последнего открытия, изменения файла и т. д.) [15, с. 43].

Анализ различных подходов к классификации позволяет отметить, что для использования с целью раскрытия и расследования преступлений электронно-цифровых следов, содержащихся на оригинальном электронно-цифровом носителе, всегда производится их перекодировка в форму, доступную для ее восприятия (отображение на экране монитора программно-технического устройства изображений, текста, динамического изображения (видео), прослушивание аудиозаписи и т. д.).

Приведенный анализ существующих точек зрения позволяет сделать следующие выводы:

рассматриваемые следы (электронно-цифровые) относятся к группе материальных следов, при этом невидимых и требующих законодательной регламентации порядка обращения с ними с целью единообразного применения норм уголовно-процессуального законодательства при работе с ними;

в основе механизма образования данных следов заложены электромагнитные взаимодействия двух и более устройств хранения, обработки и передачи электронно-цифровых данных;

следами-предметами либо следами-частями предметов рассматриваемых следов выступают электронно-цифровые носители (машинные носители информации, интегральные микросхемы, микроконтроллеры, комбинированные документы, ЭВМ, информационные системы, информационно-телекоммуникационные сети и т. д.);

для удобства восприятия и дальнейшего использования информации, которую возможно получить при анализе электронно-цифровых следов, необходимо производить их перекодировку в форму, доступную для понимания и оценки как следователем (сотрудником, осуществляющим предварительное следствие), так и иными лицами, имеющими отношение к расследованию уголовного дела.

Окончание следует

Список используемых источников

1. Белкин, Р.С. Криминалистика: проблемы сегодняшнего дня: злободневные вопросы российской криминалистики / Р.С. Белкин. – М. : НОРМА : ИНФРА-М, 2001. – 237 с.

2. Мещеряков, В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В.А. Мещеряков. – Воронеж : Изд-во Воронеж. гос. ун-та, 2002. – 408 с.

3. Агибалов, В.Ю. Виртуальные следы в криминалистике и уголовном процессе / В.Ю. Агибалов. – М. : Юрлитинформ, 2012. – 152 с.;

4. Вехов, В.Б. Основы криминалистического учения об исследования и использовании компьютерной информации и средств её обработки / В.Б. Вехов. – Волгоград : Волгогр. акад. МВД России, 2008. – 404 с.

5. Милашев, В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юрид. наук : 12.00.09 / В.А. Милашев. – М., 2004. – 22 с.

6. Мочагин, П.В. Идентификация виртуально-информационного и невербального следообразований как новое направление в криминалистике / П.В. Мочагин // Вестн. ИжГТУ. – 2013. – № 3. – С. 148–154.

7. Касаткин, А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений : дис. ... канд. юрид. наук : 12.00.09 / А.В. Касаткин. – М., 1997. – 215 л.

8. Гаврилин, Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы : дис. ... д-ра. юрид. наук : 12.00.09 / Ю.В. Гаврилин. – М., 2009. – 404 л.

9. Черкасов, В.Н. Еще раз о терминах / В.Н. Черкасов // Информ. безопасность регионов. – 2008. – № 2. – С. 70–71.

10. Лушин, Е.А. О термине «электронно-цифровые следы» / Е.А. Лушин // Сб. следств. ком. России. Расследование преступлений: проблемы и пути их решения. – 2017. – № 4. – С. 161–163.

11. Мещеряков, В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. – 2013. – № 5. – С. 265–270.

12. Вехов, В.Б. Электронные следы в системе криминалистики В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судеб. экспертиза. – 2016. – № 2. – С. 10–18.

13. Козлов, В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – М. : Горячая линия – Телеком, 2002. – 336 с.

14. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М. : Юрлитинформ, 2002. – 496 с.

15. Смушкин, А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. – 2012. – № 8. – С. 43–45.

Дата поступления в редакцию: 29.03.19

***N.N. Belomyttsev**, postgraduate student of Scientiic and Pedagogical Faculty of the Academy of the MIA of the Republic of Belarus*

FEATURES OF FORMATION OF TRACES IN COMMITTING THEFT BY MEANS OF COMPUTER TECHNOLOGY (PART 1)

The mechanism of formation is analyzed, and also existing classifications of traces of Commission of plunder by use of computer equipment are considered. Current theoretical and applied issues related to the definition of the concept of electronic-digital traces are studied, on the basis of which the use of the category «electronic-digital trace» is justified.

Keywords: electronic digital footprint, the mechanism of formation of traces, storage media of digital information.