УДК 343.985

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

СПЕЦИФИКА СЛЕДОВОЙ КАРТИНЫ ПРИ СОВЕРШЕНИИ ХИЩЕНИЯ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ: ПРАКТИЧЕСКИЙ АСПЕКТ

Предлагается общая характеристика механизма образования электронно-цифровых следов и их разновидности. Кратко описываются носители электронно-цифровой информации и предлагаются рекомендации по их использованию при расследовании уголвоного дела. Перечисляются основные действия, осуществляемые с электронно-цифровой информацией в ходе следствия. На примере рассматриваются образуемые электронно-цифровые следы при совершении хищения. Описывются постадийно преступные решения злоумышленников и используемые ими программные продукты. Обозначается взаимосвязь между электронно-цифровыми следами, способом совершения преступления и лицами, причасными к его совершению. Предлагается авторское определение электронно-цифрового следа.

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

Для науки криминалистики знания о следах любого преступного деяния выступают системообразующим обстоятельством, вокруг которого и в связи с которым формируется ее понятийный язык, ее общая и частные теории, иные подсистемы и элементы криминалистического знания.

Логично предположить, что, во-первых, дальнейшие исследования следоообразования, развитие изобретений и открытие новых способов сбора следов позволят устанавливать следы, пока недоступные следователю и специалисту, во-вторых, очевидно, что по мере улучшения методики и техники изучения следов уменьшается количество тех, которые ранее считались непригодными для каких-либо выводов [1, с. 10–11].

Исходя из общетеоретической позиции отражения, подготовка, совершение и сокрытие всяких преступных деяний, в том числе хищения путем использования компьютерной техники как конкретного события, происходящего в материальном мире, закономерно вызывают изменения в окружающей среде. Отражением преступных действий являются следы. Свойство отражения, присущее всем видам и формам материи, заключается в том, что каждый объект материального мира в процессе взаимодействия с окружающей средой подвергается воздействию внешних факторов, а следы такого воздействия сохраняются на объекте определенное время [2, с. 81].

Итак, механизм следообразования понимается как процесс взаимодействия двух и более объектов, конечная фаза которого представляет собой образование следа. Для всех способов хищений путем использования компьютерной техники такой механизм или его отдельные элементы (операции) будут общими. Основу механизма образования электронно-цифровых следов образуют электромагнитные взаимодействия также двух и более материальных объектов – объективных форм существования (представления) электронно-цифровых данных.

Взаимодействие объективных форм существования электронно-цифровой информации между собой (воздействие одного объекта следообразования на другой), как правило, устанавливается по наблюдаемому различию между тремя основными состояниями. К ним относятся содержание, формат и иные свойства, алгоритм функционирования программы, автоматически

создаваемые программой либо операционной системой скрытно от пользователей сервисные файлы, которые используются для фиксации хода обработки компьютерной информации и ее восстановления на случай какого-либо сбоя в работе программно-технического устройства или его программного обеспечения.

Фиксируемые изменения названных состояний и будут воспринимаемыми человеком следами-отображениями, характеризующими результат взаимодействия следующих объектов: электромагнитного сигнала, файла, компьютерной программы, базы данных, электронного сообщения, электронного документа, электронной страницы или сайта в компьютерной сети.

В свою очередь, следами-предметами (частями предметов) и в то же время типичными материальными носителями электронно-цифровых следов выступают электронно-цифровые (машинные) носители данных, интегральные микросхемы, микроконтроллеры, банковские платежные карточки и иные комбинированные документы, компьютеры, в том числе мобильные устройства и всевозможные гаджеты. Кроме того, в указанных технических устройствах содержится электронно-цифровая информация, связанная с событием преступления; их отдельные электронные модули при работе излучают в находящееся вокруг пространство дополнительную криминалистически значимую компьютерную информацию, которая может быть дистанционно обнаружена, зафиксирована посредством специальных программно-технических устройств (радиоэлектронные, специальные технические средства и др.). В последующем данная информация с помощью специализированных программ и устройств может быть расшифрована (раскодирована), представлена в читаемом виде для использования в процессе расследования уголовного дела [3, с. 32].

При расследовании хищений путем использования компьютерной техники проведение некоторых следственных действий включает обнаружение, фиксацию, изъятие, изучение, а также приобщение к материалам уголовного дела электронно-цифровой информации. Она изымается вместе с ее цифровым носителем либо копируется на иной цифровой носитель данных, когда невозможно или нецелесообразно изымать программно-техническое средство или сам носитель. При обнаружении, фиксации и изъятии электронно-цифровых следов у следователя либо специалиста обычно всегда есть возможность делать это выборочно из всего массива имеющихся данных. В обязательном порядке, как и при сборе любых материальных следов, не только запечатлевается сама доказательственная электронно-цифровая информация, но и фиксируется информация о путях и способах ее получения в соответствующем протоколе следственного действия как необходимое условие ее допустимости по расследуемому уголовному делу.

На практике для неоднократного использования электронно-цифровой информации в процессе расследования уголовного дела (для экспертных исследований, предъявления ее в ходе допроса и (или) судебного разбирательства и т. д.) последняя в обязательном порядке копируется и (или) сохраняется (хранится) на изъятом цифровом носителе.

К электронно-цифровым следам, образуемым при хищении путем использования компьютерной техники, в первую очередь необходимо отнести изменения исходной информации на электронно-цифровых носителях, например, следы модификации информации (текстовые файлы, базы данных, программный код и т. д.). В ходе исследования указанных носителей можно установить следы уничтожения или блокирования – размагничивание носителей, стирание или добавление отдельных файлов. Кроме того, при исследовании программно-технических устройств могут быть обнаружены следы удаленного доступа к информации с использованием глобальных или локальных компьютерных сетей. Возникновение следов обусловлено тем, что программное обеспечение устройства, имеющего доступ к той или иной сети, обычно запрашивает у иного программно-технического устройства, пытающегося с ним соединиться, некоторую техническую информацию о нем. Как правило, это IP-адрес, а при наличии системы защиты – тип и язык операционной системы, часовой пояс, название устройства, MAC-адрес, качественные характеристики дисплея и ряд других параметров программно-технического устройства, которое осуществляло доступ.

При тех или иных действиях с программно-техническими средствами, используемыми для обработки информации, кроме желаемого результата, независимо от воли пользователя, в опре-

деленных случаях автоматически формируется и иная (вспомогательная, сервисная, идентификационная и т. д.) информация. Она также имеет определенное доказательственное значение для расследования хищений путем использования компьютерной техники. Например, по реквизитам файла электронного сообщения, отправленного лицом, причастным к совершению хищения, на электронную почту потерпевшего (либо сотрудника организации, учреждения), в определенных случаях возможно установить электронный адрес почты, используемой преступником, идентификатор его программно-технического устройства (IP-адрес), MAC-адрес, производителя и модель устройства, абонентский номер этого устройства в компьютерной сети оператора связи, физический адрес нахождения устройства, с которого было отправлено сообщение, возможные следы подготовки на данном устройстве, время отправки, что может указывать на дату и время начала совершения преступления и т. д.

Показательными в этом плане являются уголовные дела в отношении группы лиц (участники международной организованной преступной группы Cobalt), совершивших хищение путем использования компьютерной техники из банкоматов белорусского ЗАО «Альфа-Банк». За несколько часов преступных действий преступники завладели 527 тыс. долларов США, 67 500 евро и почти 109 тыс. белорусских рублей из 27 банкоматов, расположенных в Минске, Могилеве и Витебске. Анализ деятельности участников преступной группы позволяет выделить ряд особенностей механизма следообразования в процессе совершения данного преступления. Изучение материалов указанных уголовных дел показало, что наиболее полно проявились закономерности образования электронно-цифровых следов [4].

Так, например, на стадии подготовки к рассматриваемому преступлению осуществлялось создание необходимых программ и подбор уже имеющихся программных продуктов. Способом проникновения в банковскую сеть послужила отправка фишингового письма с вложением, которое содержало эксплоит (программа, фрагмент программного кода или последовательность команд, которые используют уязвимости в программном обеспечении) или исполняемый файл в текстовом файле с паролем. Таким образом, на программно-технических устройствах, используемых преступниками, оставались данные программы, а также необходимый программный комплекс для создания эксплоитов и исполняемых файлов. При исследовании этих объектов внимание уделялось их версии, настройке и параметрам, которые в ряде случаев автоматически включались в исходный код создаваемой с их помощью программы (в ходе расследования программно-технические средства, на которых осуществлялась подготовка программного обеспечения, установлены и изъяты не были).

На стадии совершения преступления и проникновения в информационную систему осуществлялась отправка писем с двух серверов с установленными IP-адресами, находящимися в Российской Федерации. В компьютере получателя сообщения в log-файлах регистрировалась информация о том, кто инициировал его, когда и в какое время оно пришло, а также сам текст сообщения и файл .doc, с вшитым в него эксплоитом и исполняемыми файлами для непосредственного проникновения в информационную систему банка.

После запуска вредоносного вложения кем-либо из сотрудников (так как оно было сходно с легальным) начинался процесс его закрепления в системе, следами которого становились замененные файлы с именами iusb3mon. exe (Intel(R) USB 3.0 eXtensible Host Controller) и jusched. exe (Sun Java Update Scheduler). В результате такой замены службы, которые должны были автоматически запускать легальные программы, запускали вредоносные приложения. В тот же каталог, где находились замененные легальные исполняемые файлы, копировалась и библиотека с именем crss. dll. для загрузки из интернета модуля Beacon в оперативную память для осуществления полезной нагрузки для атакующих систему. Использовались также стандартные инструменты удаленного доступа: протокол удаленного управления Microsoft Remote Desktop Protocol либо иные инструменты удаленного доступа (модифицированный установщик TeamViewer). После успешного осуществления атаки и распространения вредоносного программного обеспечения был осуществлен доступ к программно-техническому устройству или серверу, с которого разрешен доступ к банкоматам. На последние загружалось специальное программное обеспечение eXtensions for Financial Services, которое по команде из внутренней сети банка осуществляло

процесс выдачи купюр банкоматом. Сведения и следы о данных программах были установлены в ходе следствия как на компьютерах сотрудников банка, так и на программно-технических средствах и сервере, с которого разрешен доступ к банкоматам.

После совершения преступления было осуществлено сокрытие следов преступления либо их удаление, в том числе на банкоматах, с использованием легальной и бесплатной утилиты SDelete [5]. Часть указанных следов удалось восстановить только при участии узких специалистов в области информационной безопасности.

Таким образом, на программно-технических средствах, подвергнутых атаке, были установлены следующие электронно-цифровые следы преступной деятельности: появление новых файлов (программ и их фрагментов), переименование файлов, изменение содержания файлов, их удаление и повреждение, изменение времени и даты создания файлов, их атрибутов и размеров, отсутствие доступа к информации, содержащейся в файлах (шифрование содержания, системных областей машинного носителя); помимо прочего в системном реестре операционной системы (в данном случае Windows) были указаны программы, которые были прописаны в «автозагрузке» и др. [6].

С учетом проведенного анализа можно сделать следующие выводы:

электронно-цифровые следы являются носителями информации не только об отражаемом объекте (программа, электронные сообщения и т. д.), но в некоторой степени и о способе подготовки, совершения и сокрытия преступного деяния, а через них – и о лице (лицах), причастном к совершению хищения путем использования компьютерной техники (его подготовленность, уровень профессионализма, преступные возможности и знания);

под электронно-цифровыми следами понимаются релевантные данные, представленные в форме электрических сигналов, образующих криминалистически значимую информацию, которая хранится, обрабатывается и передается с использованием программно-технических средств.

Список используемых источников

1. Шевченко, Б.И. Научные основы современной трасеологии // Осмотр места кражи, совершенной с применением технических средств : сб. науч. тр. / Б.И. Шевченко. – М. : ЛексЭст, 2004. – 104 с.

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

3. Вехов, В.Б. Способы совершения преступлений в сфере компьютерной информации и типичные следы // Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие изд. 2-е, доп. и испр. / В.Б. Вехов, В.В. Попова, Д.А. Илюшин. – М. : ЛексЭст, 2004. – 160 с.

4. Завершено расследование против мошенника, который участвовал в краже более 600 тысяч долларов у банков [Электронный ресурс]. – Режим доступа: https://finance.tut.by/news585838.html – Дата доступа: 26.03.2019.

5. Cobalt: эволюция и совместные операции [Электронный ресурс]. – Режим доступа: https://www.group-ib.ru/resources/threat-research/cobalt-evolution.html. – Дата доступа: 26.03.2019.

6. Архив суда Партизанского района г. Минска за 2018 г. – Уголовное дело № 1-16/2018.

Дата поступления в редакцию: 29.03.19

***N.N. Belomyttsev**, Postgraduate student of Scientific and Pedagogical Faculty of the Academy of the MIA of the Republic of Belarus*

THE SPECIFICS OF THE TRACE PATTERN IN THE THEFT USING COMPUTER TECHNOLOGY: A PRACTICAL ASPECT

A general characteristic of the mechanism of formation of electronic-digital traces is proposed, some of which are considered as examples by example. Carriers of electronic-digital information are briefly described and recommendations are given for their use in investigating a corner case. The main actions carried out with electronic digital information during the investigation are listed. The example examines the generated electronic-digital traces during the theft. It describes the stepwise criminal decisions of attackers and the software products they use. The relationship between electronic-digital tracks, the method of committing a crime and the persons involved in its commission is indicated. The author's definition of an electronic digital trace is proposed.

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