методологическое обеспечение следственной профилактики уже давно не отвечает современным реалиям, а необходимость изучения теоретических основ криминалистической профилактики обусловливается и тем, что отдельные исследователи периодически предпринимают малопродуктивные попытки пересмотра традиционной системы криминалистики.

В связи с этим процесс становления учения о криминалистической профилактике преступлений позволит укрепить фундаментальные основы криминалистики и реализовать ее не использованные до сих пор потенциальные возможности в разработке эффективных средств и методов предупреждения преступлений.

УДК 343.98

И.В. Пашута

НЕКОТОРЫЕ АСПЕКТЫ ЦИФРОВЫХ СЛЕДОВ В КРИМИНАЛИСТИКЕ

Значительный рост преступлений, связанных с использованием правонарушителями информационно-телекоммуникационных технологий, потребовал, с одной стороны, выработки действенных мер реагирования со стороны правоохранительных органов, а с другой – послужил интенсификации научных исследований, направленных на совершенствование деятельности органов уголовного преследования по раскрытию, расследования и предупреждению преступлений в данной сфере.

В этой связи в теории криминалистики наблюдается тенденция изучения так называемых цифровых (виртуальных, компьютерных, электронных) следов преступной деятельности, под которыми многие ученые (А.М. Багмет, Д.В. Бахтеев, В.В. Бычков, В.Б. Вехов, Н.Н. Ильин, С.Ю. Скобелин и др.) понимают криминалистически значимую компьютерную информацию, т. е. сведения (сообщения, данные), представленные в форме электронных сигналов, независимо от средств их хранения, обработки и передачи.

Указывая на особую природу исследуемых следов, В.А. Мещеряков отмечает, что в основе механизма их формирования лежит специфическое цифровое отображение, происходящее в искусственно созданной среде – канале связи, информационной системе, информационно-телекоммуникационной сети, памяти иных электронных носителей информации. При формировании цифровых следов на материальном носителе фиксируются не сами свойства наблюдаемого физического процесса (звук, видеоролик и т. п.), а всего лишь цифровые значения параметров формализованной математической модели, положенной в основу технического устройства регистрации его реального проявления. В то же время такой след представляет собой сложную информационную структуру, в которой содержится значительный объем вспомогательных данных, отвечающих за его целостность и возможность восприятия с помощью соответствующих программно-технических средств.

Физически не имея целостной структуры, цифровой след может состоять из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких электронных носителях информации, подключены как к одному, так и к нескольким (возможно территориально расположенным на значительных расстояниях) компьютерам, объединенным в информационную систему или информационно-телекоммуникационную сеть. При этом структура получаемого в каждый конкретный момент цифрового следа может зависеть как от технических особенностей регистрирующего компьютерного устройства в целом, так и от его текущего состояния.

Особое практическое значение имеют материальные электронные носители цифровых следов, без которых последние не могут существовать физически. Анализ специальной литературы позволяет все многообразие электронных носителей цифровых следов разделить на следующие группы.

1. Оконченные устройства. К ним, по мнению А.Г. Волеводза, А.Ю. Семенова и других ученых, относятся следы на машинных носителях (жесткий диск, ферромагнитная полимерная лента или полоса, ферромагнитная металлическая нить; магнитная лента (стример), жесткий оптический или магнитооптический диск (CD, DVD)); микроконтроллере – программно управляемом микроэлектронном устройстве (SIM-карта, карта памяти (флеш-карта), так называемые USB-драйверы и др.); в оперативных запоминающих устройствах компьютера, периферийных устройств (принтер, сканер и др.).

Более подробно следует остановиться на цифровых следах, остающихся на компьютере преступника и потерпевшего, где прежде всего анализируются таблица расширения файлов (FAT, NTFS или другая в зависимости от типа используемой операционной системы); системный реестр операционной системы; отдельные кластеры магнитного носителя информации (жесткий диск, дискета), в которых записываются фрагменты исполняемых файлов (программ) и файлов конфигурации; файлы и каталоги (папки) хранения входящей электронной почты и прикрепляемых исполняемых файлов, конфигурации почтовой программы; файлы конфигурации программ удаленного соединения компьютера с информационной сетью.

Рассматривая отображение в памяти компьютера любых действий с компьютерными или иными программируемыми устройствами (мобильный телефон, цифровой плеер, часы, браслеты, планшеты и т. д.), А.Б. Самушкин указывает на следующие цифровые следы: включение, выключение, различные операции с содержимым памяти компьютера (отображаются в журналах администрирования, безопасности, приложений и т. д.); действия с наиболее важными для работы компьютера программами (установка, удаление и т. д.), отражаемыми в реестре компьютера (reg-файлах); сведения о работе в сети Интернет, локальных и иных сетях, содержащихся в log-файлах, истории журналов браузеров пользователя; операции с файлами (отражаются в их свойствах, например, время создания, последнего открытия, изменения файла и др.).

2. Промежуточные устройства. Среди них выделяются следы, остающиеся в коммутаторе (сведения о подключаемых устройствах, содержащихся в таблице MAC-адресов), маршрутизаторе (используется для передачи трафика между различными сетями), межсетевом экране (предназначен для фильтрации локального и входящего трафика).

Цифровые следы могут послужить доказательствами незаконного проникновения в память компьютера или иного устройства, совершения или планирования преступления с использованием информационно-телекоммуникационных технологий конкретным лицом (группой лиц).

Преступлениям в сфере информационных технологий свойственна предварительная подготовка, написание и приобретение специальных программ для взлома, внедрение троянских программ, поиск паролей или определение способов беспарольного входа и т. д. Написание или тестирование подобных программ будет оставлять цифровые следы на компьютере правонарушителя. В свою очередь, способ проникновения в память компьютера (иного устройства) путем подбора пароля случайным образом или с помощью специальных компьютерных программ, активизации троянов и т. д., а также способ сокрытия следов оставляют отражение в памяти компьютера потерпевшего.

Таким образом, можно сделать следующие выводы.

Цифровой след представляет собой криминалистически значимую компьютерную информацию (сведения, сообщения, данные), представленную в форме электронных сигналов.

В основе механизма его формирования лежит специфическое цифровое отражение, происходящее в искусственно созданной среде – канале связи, информационной системе, информационно-телекоммуникационной сети, памяти иных электронных носителей информации. Цифровой след имеет сложную информационную структуру, в которой помимо внешне выраженной информации содержится значительный объем вспомогательных данных, отвечающих за его целостность и возможность восприятия с помощью соответствующих программно-технических средств. Такой след не может физически существовать без материального электронного носителя.

Электронные носители цифровых следов, по нашему мнению, следует разделить на оконченные и промежуточные устройства. Их криминалистическое исследование во многом способствует установлению различных обстоятельств, имеющих значение для раскрытия, расследования и предупреждения преступлений, связанных с использованием информационных технологий.

УДК 343.98

Н.Н. Пашута

О КРИМИНАЛИСТИЧЕСКОМ ОБЕСПЕЧЕНИИ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ПОДРАЗДЕЛЕНИЙ УГОЛОВНОГО РОЗЫСКА КРИМИНАЛЬНОЙ МИЛИЦИИ ПРИ ПРОВЕДЕНИИ ПРОВЕРКИ ПО ЗАЯВЛЕНИЯМ И СООБЩЕНИЯМ О ПРЕСТУПЛЕНИИ

В соответствии со ст. 37 УПК Республики Беларусь МВД Республики Беларусь территориальные органы внутренних дел являются органами дознания, на которые возлагается решение ряда задач в рамках производства по материалам и уголовным делам: прием, регистрация и рассмотрение заявлений и сообщений о любом совершенном, совершаемом и готовящемся преступлении; проведение проверки по заявлению или сообщению о преступлении, принятие по ним решения в соответствии со ст. 174 УПК Республики Беларусь; проведение необходимых оперативно-розыскных мероприятий и принятие иных мер в целях обнаружения преступлений и выявления лиц, их совершивших, установления похищенного имущества и др.

Лицо на стадии возбуждения уголовного дела не только выявляет признаки преступления либо их отсутствие, но и получает фактические сведения о происшедшем, выдвигает первоначальные версии, определяет пути дальнейших действий. Активность и профессиональное мастерство сотрудников органов дознания при реализации своих функциональных полномочий при проведении проверки по заявлениям и сообщениям о преступлении в порядке уголовно-процессуального законодательства Республики Беларусь становятся существенным фактором в реализации принципа неотвратимости наказания за совершенное преступление.

Анализ статистических данных информационного центра МВД Республики Беларусь свидетельствует о том, что за 9 месяцев 2021 г. органами внутренних дел Республики Беларусь более чем по 50 % рассмотренных заявлений и сообщений о преступлении принято решение об отказе в возбуждении уголовного дела, по которым в 15 % случаев такое решение отменено прокурором и направлено на дополнительную проверку. Примерно в 100 случаях решения об отказе в возбуждении уголовного дела отменены прокурорами с одновременным возбуждением уголовного дела. При этом необходимо отметить, что более 90 % заявлений и сообщений о преступлениях рассмотрено сотрудниками уголовного розыска криминальной милиции и участковыми инспекторами милиции общественной безопасности.

Изучение отмененных прокурором решений по материалам проверок, разбирательство по которым проведено сотрудниками уголовного розыска криминальной милиции, указывает на то, что основными причинами возврата материалов для дальнейшей проверки служит непринятие надлежащих мер по всестороннему, полному и объективному исследованию обстоятельств, содержащихся в материалах проверки, неполнота проведенных проверок. Названные обстоятельства препятствуют получению данных о конкретных признаках преступления, не позволяют принять решение о возбуждении уголовного дела. Так, анализ самих материалов проверок свидетельствует о единичных случаях применения технико-криминалистических средств, приемов и методов для обнаружения следов, предметов (объектов), имеющих значение для установления всех обстоятельств проверяемого события. В основном они использовались для фотофиксации хода и результатов следственных действий, производство которых возможно до принятия решения о возбуждении уголовного дела.

При этом необходимо отметить, что руководство МВД Республики Беларусь регулярно обращает внимание на необходимость качественного, всестороннего и полного проведения сотрудниками органов внутренних дел разбирательства по