УДК 343.9

А.И. Чурносов

ОСОБЕННОСТИ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ ЦИФРОВЫХ СЛЕДОВ ПРИ ПРОИЗВОДСТВЕ ДОЗНАНИЯ ПО ПРЕСТУПЛЕНИЯМ ПРОТИВ ПОГРАНИЧНОЙ БЕЗОПАСНОСТИ

В современный период для должностных лиц органов пограничной службы (ОПС) все более актуальным становится использование цифровых следов при расследовании преступлений, создающих угрозу пограничной безопасности, в первую очередь по уголовным делам, возбуждаемым по признакам преступлений, связанным с организацией незаконной миграции (ст. 371[1] Уголовного кодекса Республики Беларусь), незаконным перемещением через таможенную границу Евразийского экономического союза и (или) Государственную границу Республики Беларусь наркотических средств, психотропных веществ либо их прекурсоров или аналогов (ст. 328[1] Уголовного кодекса Республики Беларусь), и некоторых других [1].

Вместе с тем за пределами научной проработки остались вопросы обнаружения, фиксации и изъятия необходимой компьютерной информации и технических средств ее обработки. Отсутствие рекомендаций по рассматриваемому вопросу в ОПС, несомненно, порождает возникновение все новых проблем при расследовании преступлений, сопряженных с использованием ресурсов сети Интернет, и фиксации доказательственной информации, хранящейся на электронных носителях и на ресурсах сети Интернет. Прежде всего это касается вопросов противоправного финансирования незаконного перемещения физических лиц, транспортных средств и товаров через Государственную границу Республики Беларусь. С учетом отсутствия прямых контактов участников таких преступлений используются дистанционные связи посредством сети Интернет. Изложенное обусловливает необходимость рассмотрения проблем обнаружения и фиксации цифровых следов, при производстве дознания по преступлениям, создающим угрозу пограничной безопасности.

Выявление преступлений, совершаемых посредством сети Интернет, требует технических (отраслевых), теоретических знаний по выявлению и фиксации цифровых следов, сформированных криминалистической наукой, и практических навыков, полученных в результате раскрытия, расследования преступлений и опыта работы в сетевом пространстве. При этом к цифровым следам следует относить данные о совершении действий в информационном пространстве технических устройств, их сетей и систем, такие как создание, включение, удаление, внесение изменений, активация, открывание.

Преступники, обладающие значительными знаниями в области работы интернет-технологий и интернет-систем, могут подставлять под уголовную ответственность непричастных лиц, зная десятки различных способов, самыми распространенными из которых являются подмены IP-адресов правонарушителя на адрес законопослушного гражданина. В связи с этим при сборе и фиксации доказательственной информации лицо, производящее дознание в ОПС, изначально должно понимать, что цифровые следы, отражающиеся в IP-адресе рассылки, впоследствии будут лежать в основе обвинения. Действия лиц, совершающих преступления и скрывающих их подобным образом, очень сложно доказать, что подтверждается многочисленной судебной практикой. Сущность описанной проблемы заключается в следующем: лица, совершающие преступления, производят все операции с подконтрольными им счетами и аккаунтами с использованием специализированного программного обеспечения, позволяющего производить обращение к ресурсам через серверы, расположенные за территорией Республики Беларусь. В таком случае операторы ресурса в сети Интернет фиксируют IP-адрес прокси-сервера, а не лица, отправившего конкретную команду. Выходом из подобной ситуации является направление запроса об оказании правовой помощи в страну, в которой зарегистрирован провайдер, с IP-адреса которого передана команда на проведение операции, с целью выяснения сведений об IP-адресе обращения к серверу, который может быть истинным адресом преступника.

Преступниками может быть осуществлена также подмена MAC-адреса, так как скрыть его наличие в сети Интернет невозможно, его с легкостью меняют как средствами операционных систем, например через реестр или настройки драйвера, так и с помощью специальных программных утилит. Целесообразно учитывать, что фактически MAC-адрес устройства не изменяется, потому что это физический адрес устройства; меняется так называемый программный физический адрес устройства, но для злоумышленников этого достаточно, чтобы стать анонимными в сети Интернет. Понять, использует злоумышленник настоящий или «фиктивный» MAC-адрес, можно непосредственно при осмотре устройства. С этой целью необходимо сравнить адрес, выводимый системой, и адрес, указанный на самом устройстве, или же воспользоваться любой утилитой для тестирования ПК, например Everest или Astra.

Указанная анонимность позволяет быть неизвестным пользователем сети Интернет и при совершении финансовых операций, и при обращении электронных денег. В последнее время все большее распространение и популярность в сетевом пространстве набирают системы хранения и передачи валют, это так называемые электронные деньги, которые можно перечислить на счета различных платежных систем.

В обобщенном виде подход зарубежного законодательства выглядит так, что, с одной стороны, электронные деньги представляют собой особые средства обращения традиционных и частных валют, которые используются для упрощения финансовых расчетов при оплате товаров и услуг в сети Интернет, с другой – обязательства эмитента, которые исполняются в традиционных, не электронных деньгах [2, с. 96–97].

Сеть Интернет представляет собой всемирную информационную компьютерную сеть, именуемую в повседневном общении – мировой паутиной. Она аккумулирует огромное количество компьютерных сетей, работающих по единым правилам, и включает пользователей почти из всех стран мира. Однако единство правил относится в значительной степени к технической составляющей, чем к правовой, поскольку по целому ряду правовых вопросов нет международного единства мнений. В связи с этим перед лицами, производящими дознание в ОПС, стоит задача: производить дознание по преступлениям, создающим угрозу пограничной безопасности, совершенным с использованием сети Интернет, опираясь на национальное законодательство, но в рамках международного взаимодействия учитывать и законодательство страны, с которой необходимо осуществлять международное сотрудничество, направленное на фиксацию доказательств в рамках расследования уголовного дела. Анализ уголовных дел по преступлениям данной категории свидетельствует о том, что преступления имеют межрегиональный и международный характер, что также негативно сказывается на результатах расследования уголовных дел по причине «запаздывания» производства следственных действий и их фиксации. При фиксации доказательственной информации, хранящейся на ресурсах сети Интернет, лицу, производящему дознание, необходимо учитывать уголовно-процессуальные нормы, общие криминалистические рекомендации, технические особенности работы компьютерных систем и сетевого интернет-пространства.

Фиксация доказательственной информации, содержащей цифровые следы, должна быть представлена в виде последовательной и полной цепи отраженных в процессуальных документах сведений, замкнутых по смыслу. В качестве таких процессуальных документов целесообразно рассматривать протоколы осмотра смартфонов, ноутбуков и других гаджетов.

В современный период при совершении преступлений, создающих угрозу пограничной безопасности, в первую очередь организация незаконной миграции, незаконное перемещение через таможенную границу Евразийского экономического союза и (или) Государственную границу Республики Беларусь наркотических средств, психотропных веществ

либо их прекурсоров или аналогов и других, лицами, совершающими данные преступные деяния, активно используются современные информационные технологии, позволяющие скрывать личность, а также следы совершаемых преступлений. Вместе с тем развитие криминалистической техники и тактики позволяет обнаруживать и фиксировать цифровые следы, которые остаются в данном случае. Вышеизложенное обусловливает активное использование лицами, производящими дознание в ОПС, положений нового раздела криминалистической техники, как «форензика» для решения задач при расследовании преступлений.

При расследовании преступлений, создающих угрозу пограничной безопасности, при совершении которых используются информационные технологии, чаще используется проведение такого следственного действия, как осмотр смартфонов, ноутбуков и других гаджетов. В процессе его осуществления с большой вероятностью может быть осуществлено обнаружение цифровых следов, с последующей их фиксацией, изъятием и использованием при расследовании по уголовным делам. Фиксация содержания цифровых следов предполагает отображение последовательной и полной цепи ее отражения в виде сведений, замкнутых по смыслу, в таких процессуальных документах, как протоколы осмотра смартфонов, ноутбуков и других гаджетов.

1. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : в ред. Закона Респ. Беларусь от 13.05.2022 г. № 165-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети интернет : автореф. дис. ... канд. юрид. наук : 12.00.12 / А.Н. Колычева ; Рос. гос. ун-т правосудия. – М., 2018. – 199 с.

УДК 343.985.7

Ю.М. Юбко

ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ ДОКАЗЫВАНИЮ ПО МАТЕРИАЛАМ И УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Процессуально закрепленные следы являются носителями информации, позволяющей установить обстоятельства, подлежащие доказыванию в соответствии с требованиями ст. 89 и 90 Уголовно-процессуального кодекса Республики Беларусь (УПК), так как данные нормы явля-