ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА

Пацкевич А. П., Белов Д. Н.

Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, lawcrim@bsu.by

В статье исследуются вопросы использования информационных технологий на первоначальном этапе расследования мошенничества с учетом имеющихся современных достижений. Обосновывается необходимость совершенствования материально-технической базы или технико-криминалистических средств борьбы с мошенничеством, исследуются наиболее эффективные средства работы с цифровыми следами. Предлагаются рекомендации по повышению эффективности отдельных следственных и иных процессуальных действий.

Рассматривается возможность создания автоматизированной системы криминалистических учетов по способу совершения преступления, позволяющая создавать информационную модель преступления на основе имеющейся в системе информации, что особенно важно на первоначальном этапе расследования преступлений, в том числе и мошенничества, в условиях отсутствия информации о лице, совершившем преступление.

Ключевые слова: информационные технологии; цифровые следы; цифровое мошенничество; способ совершения преступлений; следственный осмотр; средства работы со следами

В современном мире, где цифровая трансформация общества затронула многие сферы его жизнедеятельности, такое преступление как мошенничество можно признать одним из самых опасных видов хищений, что объясняется не только высоким интеллектуальным развитием лиц, его совершающих, появлением новых способов его совершения, к которым можно отнести, в частности «фишинг», «вишинг» и другие, связанные с использованием информационных технологий (далее – ИТ), но и необходимостью совершенствования материально-технической базы или технико-криминалистических средств борьбы с ним. Таковыми, в свою очередь, должны стать те, что в основе принципов работы предполагают использование современных информационных технологий.

Согласно статье 1 Закона Республики Беларусь от 10 ноября 2008 г. № 445-З «Об информации, информатизации и защите информации» под информационной технологией понимается совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации. Как видно из представленного определения понятия «информационная технология», оно предполагает достаточно широкий перечень возможных действий, осуществляемых с информацией, производство которых позволяет говорить о том или ином явлении как об информационной технологии, что дает нам основание причислять к таковым различного рода средства работы с цифровыми следами, а также криминалистические учеты, о чем будет сказано ниже.

Следователь, лицо, производящее дознание, сталкиваются с информационными технологиями при расследовании мошенничеств уже на этапе проведения первоначальных следственных и иных процессуальных мероприятий, поскольку необходимо определиться с вопросом о том, какие из них целесообразно произвести на данном этапе, особенно по делам о т.н. «цифровых мошенничествах» в условиях полного отсутствия значимой информации. В свою очередь, от этого зависит эффективность всей работы в целом на первоначальном этапе расследования в контексте возможности достижения основной цели в виде установления лица, совершившего преступление.

Определение объема необходимых для проведения конкретных мероприятий зависит от той типичной следственной ситуации, которая сложилась на этапе построения алгоритма действий следователя, лица, производящего дознание. Классификация следственных ситуаций осуществляется по различным критериям: 1) по процессуальному статусу субъекта, обнаружившего преступление (В.В. Крылов) [1, с. 235]; 2) по способу совершения преступления (А.В. Остроушко) [2, с. 104-105]; 3) по степени информационной определенности (Ю.В. Гаврилин, А.В. Кузнецов) [3, с. 101, 110].

Наибольший интерес для нас представляет классификация, данная А.Н. Яковлевым и Н.В. Олиндер в своем научно-практическом пособии 2012 года «Особенности расследования преступлений, совершаемых с использованием электронных платежных средств и систем», где предложено разделить типичные следственные ситуации по всем «цифровым преступлениям» на две группы: 1) известен факт совершения преступления и необходимо установить лицо, его совершившее, 2) известен как факт совершения преступления, так и лицо, его совершившее [4, с. 80]. Для процесса расследования мошенничества на его первоначальном этапе криминалистический интерес представляет та типичная следственная ситуация, которая предполагает необходимость установления лица, совершившего такое мошенничество, что объясняется возникающими сложностями в расследовании в контексте производства следственных и иных процессуальных действий: следственного осмотра, допроса потерпевшего, направления запросов и назначения экспертиз.

Следственный осмотр. Так, одним из существенных мероприятий на первоначальном этапе расследования «цифрового мошенничества» следует назвать следственный осмотр.

Исходя из сущности совершаемых действий, составляющих «цифровое мошенничество», на наш взгляд, нет необходимости в проведении такого вида следственного осмотра как осмотр места происшествия, поскольку само преступление совершается в цифровом пространстве, отсутствует и само место происшествия в его классическом понимании. В таких случаях действенным механизмом, позволяющим заменить осмотр места происшествия, будет производство обыска или выемки с последующим следственным осмотром обнаруженного, предъявленного (осмотр вещей, предметов, документов, компьютерной информации).

Несмотря на имеющееся многообразие способов совершения как мошенничества в целом, так и «цифрового мошенничества», можно выделить некоторые

рекомендации, единые для лиц, его производящих в контексте особенностей обнаружения и изъятия «цифровых» следов, на наш взгляд, позволяющие повысить эффективность данного следственного действия:

привлечение специалиста для производства осмотра при работе с «цифровыми следами», их обнаружения, закрепления и изъятия;

использование современных технико-криминалистических средств, предполагающих возможность обнаружения и изъятия следов преступления при проведении следственного осмотра;

наличие у следователя, лица, производящего дознание соответствующих специальных знаний, позволяющих повысить результативность следственного осмотра.

Использование современных технико-криминалистических средств дает возможность осуществлять обнаружение, закрепление, сохранность «цифровых» следов без их возможного уничтожения и (или) изменения.

Так, следует упомянуть наиболее эффективные из имеющихся в практической деятельности следственных и оперативных подразделений различных государств, используемые при проведении осмотров средства работы с «цифровыми» следами, к которым можно отнести следующие: Cellebrite UFED, MSAB XRY, «Мобильный Криминалист», Rusolut, Magnet AXIOM, Belkasoft Evidence Center, X-Ways Forensics, Elcomsoft Mobile Forensic Bundle, ACELab.

Остановимся на функциональных особенностей некоторых из них. Так, Cellebrite UFED в различных своих модификациях позволяет работать с данными из различных мобильных устройств, включая: извлечение данных с возможностью взлома устройства путем ввода соответствующего графического ключа, пароля или кода и их декодирования, выполнять восстановление удаленных данных в памяти устройства; обнаружить вредоносное ПО (вирусные программы и иное); выполнить расшифровку, т.е. преобразование обнаруженной информации на устройстве в читаемый, удобный вариант, а также извлекать и анализировать личные данные из социальных сетей и мессенджеров; извлекать информацию из различных облачных источников хранения информации, а также выполнять иные технические функции, позволяющие облегчить работу с обнаруженной и изъятой информацией. MSAB XRY имеет возможность извлечения и анализа информации из различного рода устройств (мобильные телефоны, планшеты и т.д.).

«Мобильный Криминалист» позволяет извлекать и анализировать данные из мобильных устройств, а также SIM и SD-карт; извлекать и расшифровывать данные облачных сервисов Google, Apple Maps, Facebook и др.; осуществлять анализ связей между владельцами мобильных устройств и их контактами, между несколькими устройствами через анализ звонков, SMS и MMS сообщений, электронной почты, Skype и др.; извлекать географические координаты из мобильных устройств, облачных сервисов и т.д.; осуществлять иные функции.

К функциям Magnet AXIOM относятся извлечение и анализ данных из мобильных устройств, а также жестких дисков и различного рода накопителей, облачных хранилищ; исследование устройств, извлечение скрытых файлов и восстановление удаленных данных; установление вредоносного программного обеспечения и др. X-Ways Forensics позволяет извлекать и анализировать ин-

формацию с жестких дисков, электронной почты, истории веб-браузеров, журналов ОС Windows [5, с. 169].

Все эти программные продукты позволяют следственным и оперативным подразделениям эффективно осуществлять процесс расследования и раскрытия цифровых преступлений, в том числе и «цифрового мошенничества».

Закономерной тенденцией последних лет является унификация имеющегося функционала у средств работы с цифровыми следами, которая проявляется в том, что разработчики указанных средств совмещают в них возможности исследования различного рода объектов (от мобильных устройств до облачных хранилищ), а также увеличивают количество функций программы (например, не только анализ и декодирование информации, но и поиск вредоносного программного обеспечения). В свою очередь, данная тенденция также повышает эффективность процесса расследования «цифровых преступлений».

Допрос потерпевшего. Допрос потерпевшего на первоначальном этапе расследования мошенничества имеет определяющее значение, поскольку во многих случаях именно потерпевший сообщает о совершенном преступлении, при этом его показания могут достаточно продолжительное время оставаться единственным источником сведений об обстоятельствах произошедшего. При допросе потерпевшего по данной категории дел следует учитывать следующее:

механизм совершения «цифрового мошенничества» предполагает использование мошенником специальных навыков и умений, а потому потерпевший в силу отсутствия таковых может объясняться т.н. «просторечиями», сообщая при этом не имеющие значения для расследования факты, и умышленно или по неосторожности упуская важные обстоятельства, кажущиеся ему несущественными;

потерпевшими по таким делам зачастую являются социально уязвимые категории граждан: пенсионеры, инвалиды и т.д., т.е. лица, подверженные в большей степени внушаемости, обману и т.п., что также накладывает своеобразный отпечаток на процесс допроса.

Изложенное выше свидетельствует о том, что, на наш взгляд, необходимо тщательно готовиться к допросам потерпевших по таким уголовным делам, учитывая физиологические, психологические и иные особенности потерпевших, так как это позволит обеспечить проведение качественного допроса, что, в свою очередь, даст точное направление для дальнейшего расследования.

Направление запросов и назначение экспертиз. Следует отметить, что направление запросов и назначение экспертиз не могут быть корректно выполнены без производства таких следственных действий, как осмотр и допрос потерпевшего, так как последние помогают определить предмет запроса или экспертизы. Иначе говоря, чтобы направить запрос или составить постановление о назначении экспертизы, необходимо точно сформулировать требования о предоставлении конкретной информации (особенно в запросах о международной правовой помощи по делу), либо поставить конкретные, входящие в компетенцию эксперта, имеющие отношение к делу, вопросы, подлежащие разрешению.

К запрашиваемой информации можно отнести: сведения о телефонных соединениях конкретного абонента по номеру, сведения об интернет-соединениях, получение конкретного IP-адреса с которого был отправлен запрос в сеть, и т.д.,

что стало возможным также благодаря внедрению различного рода информационных технологий.

Исходя из своеобразных способов совершения «цифровых мошенничеств», а также наличия под влиянием особенностей механизма следообразования «цифровых следов» на первоначальном этапе расследования указанных уголовных дел, наиболее часто проводятся компьютерно-техническая экспертиза и экспертиза радиоэлектронных устройств, под которыми можно понимать «самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических экспертиз, проводимый в целях определения статуса объекта, выявления и изучения его роли в преступлении, а также получения доступа к информации на электронных носителях с последующим всесторонним ее исследованием» [6, с. 118].

Еще одним важным аспектом расследования мошенничеств является накопление и сбор значимой криминалистической информации о совершенных преступлениях, в том числе сходных между собой по способу их совершения, а также ее проверка по различным учетам. Как уже отмечалось выше, мошенничество совершается разнообразными способами, которые при этом постоянно совершенствуются, что в свою очередь затрудняет процесс их эффективного расследования и раскрытия.

Исторически борьба с преступностью потребовала принятия определенных мер для обеспечения расследования и раскрытия преступлений. Данные меры включали, в том числе и разработку методов регистрации правонарушителей и совершаемых ими деяний, отсутствие регистрации которых делало практически невозможным ведение организованной борьбы с преступностью. Одним из таких методов регистрации (учетов) является криминалистический учет по способу совершения преступлений, который представляет собой форму регистрации преступлений по определенным устойчивым признакам, характеризующими механизм совершения преступления и личность преступника.

На наш взгляд, необходимо вместо существующих в Республике Беларусь автоматизированных баз данных разработать единую автоматизированную поисковую систему, которая будет по запросу в каждом конкретном случае выдавать информационную модель преступления, в которой найдут свое отражение такие элементы (их подробное описание), как: 1) объект и предмет преступного посягательства; 2) орудие и (или) средства совершения преступления; 3) следовая картина, как классические материальные и идеальные следы, так и цифровые; 4) способ совершения преступления; 5) личность преступника.

Работа указанной системы предполагается на основе аккумулирования уже внесенной и постоянно дополняющейся информации об указанных выше элементах применительно к конкретному преступлению, осуществлении анализа по результатам запроса и выдачи конкретной информации с вероятностным (а в некоторых случаях и точным – все зависит от полноты введенных в запрос сведений по различным параметрам) выводам с применением в своей основе математических методов, а также современных способов хранения, анализа, получения и защиты имеющейся информации. Значение данной модели будет заключаться в том, что она будет выступать определенной основой для построения различных общих и частных версий по делу и планирования расследования; иметь особую

практическую ценность в условиях недостатка информации на первоначальном этапе расследования преступлений, особенно мошенничеств, где, в большинстве случаев, сведений о лице, его совершившем, не имеется.

Таким образом, исследовав вопросы использования информационных технологий на первоначальном этапе расследования мошенничества, можно сделать следующие выводы.

Одной из важной задач первоначального этапа расследования мошенничества является решение вопроса о том, какие из следственных и иных процессуальных действий целесообразно произвести на данном этапе, поскольку от этого зависит эффективность всей работы в целом на первоначальном этапе расследования в контексте возможности достижения основной цели в виде установления лица, совершившего преступление.

На наш взгляд, можно выделить некоторые рекомендации, единые для лиц, его производящих в контексте особенностей обнаружения и изъятия «цифровых» следов, позволяющие повысить эффективность данного следственного действия:

1) привлечение специалиста при работе с «цифровыми следами» для их обнаружения, закрепления и изъятия;

2) использование современных технико-криминалистических средств;

3) наличие у следователя, лица, производящего дознание, специальных знаний, позволяющих повысить результативность следственного осмотра.

Использование современных технико-криминалистических средств (средств работы с «цифровыми» следами) к которым можно отнести следующие: Cellebrite UFED, MSAB XRY, «Мобильный Криминалист», Rusolut, Magnet AXIOM, Belkasoft Evidence Center, X-Ways Forensics, Elcomsoft Mobile Forensic Bundle, ACELab. дает возможность осуществлять обнаружение, закрепление, сохранность «цифровых» следов без их возможного уничтожения и (или) изменения.

Допрос потерпевшего на первоначальном этапе расследования мошенничества имеет определяющее значение, поскольку во многих случаях его показания могут достаточно продолжительное время оставаться единственным источником сведений об обстоятельствах произошедшего, необходимо тщательно готовиться к допросам потерпевших по таким уголовным делам, учитывая физиологические, психологические и иные особенности потерпевших.

Взаимосвязь таких мероприятий, как направление запросов и назначение экспертиз и таких следственных действий, как осмотр и допрос потерпевшего, проявляется в том, что последние помогают точно сформулировать требования о предоставлении конкретной информации (особенно в запросах о международной правовой помощи по делу) либо поставить конкретные, входящие в компетенцию эксперта, имеющие отношение к делу, вопросы, подлежащие разрешению.

По нашему мнению, все вышеизложенное позволит более эффективно раскрывать и расследовать совершенные мошенничества в кратчайшие сроки.

Библиографический список

1. Крылов, В. В. Расследование преступлений в сфере информации / В. В. Крылов. – М.: изд-во «Городец», 1998. – 264 с.

2. Остроушко, А. В. Организационные аспекты методики расследования преступлений в сфере компьютерной информации : автореф. дис. ... канд. юрид. наук : 12.00.09 / А. В. Остроушко ; Волгоградский юрид. ин-т МВД России. – Волгоград, 2000. – 18 с.

3. Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / Ю. В. Гаврилин [и др.] ; под ред. Ю.В. Гаврилина. – М.: Книжный мир, 2003. – 245 с.

4. Олиндер, Н. В. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: науч.-метод. пособие / Н. В. Олиндер, А. Н. Яковлев. – М.: Следственный комитет, 2012. – 144 с.

5. Гаспарян, Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: дис. ... канд. юрид. наук : 12.00.12 / Г. З. Гаспарян. – М., 2020. – 300 л.

6. Россинская, Е. Р. Судебная компьютерно-техническая экспертиза / Е. Р. Россинская, А. И. Усов. – М.: Право и закон, 2001. – 416 с.

ИСПОЛЬЗОВАНИЕ СПОСОБА СОВЕРШЕНИЯ И СОКРЫТИЯ ПРЕСТУПЛЕНИЯ В ЮРИДИЧЕСКИХ НАУКАХ

Пацкевич А. П., Чжу Цзюй Чжен

Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, lawcrim@bsu.by

В данной статье исследуется использование данных о способе совершения и сокрытия преступлений в юриспруденции на примере наук: уголовного права, уголовного процесса и криминалистики. В уголовном праве данная дефиниция нашла свое применение как один из элементов субъективной стороны состава преступлений. В уголовном процессе способ совершения преступления рассматривается как обстоятельство, устанавливаемое и доказываемое при расследовании уголовного дела и при предъявлении виновному лицу обвинения. В криминалистике данное понятие рассматривается как элемент реалистической характеристики любого вида и группы преступлений. При этом анализируются различные подходы к дефиниции способа совершения преступления со стороны различных ученых.

Ключевые слова: способ совершения и сокрытия преступления; элемент криминалистической характеристики

Рассматривая понятие способа совершения и сокрытия преступлений в юридических науках, следует отметить, что большинство криминологов и специалистов в уголовном праве (В.А. Бугаев, Н.Ф. Кузнецов, В.Н. Кудрявцев, М.В. Шкеле) [1, с. 110-114; 2, с. 38-47; 3, с. 72; 4, с. 25-27] определяют способ совершения преступления как факультативный признак объективной стороны состава преступления. В то же время ряд авторов возражают против этого и причисляют его к числу обязательных признаков объективной стороны состава преступления (Г.Г. Зуйков, А.В. Самойлов, Г.А. Густов), указывая, что «он характерен для каждого преступления и во многих случаях важен при квалификации преступления» [5, с. 22; 6, с. 28-32; 7, с. 80-87].