КЛИМОВА Я.А.,
кандидат юридических наук, профессор кафедры криминалистики учебно-научного комплекса по предварительному следствию в органах внутренних дел Волгоградской академии МВД России
aya3008@yandex.ru

УДК 343.985.7

ОСОБЕННОСТИ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Расследование преступлений, методика расследования, IT-технологии, информационно-телекоммуникационные технологии, Интернет, цифровизация, цифровые доказательства.

В статье анализируются статистические данные по преступлениям, совершенным с использованием информационно-телекоммуникационных технологий. Делается вывод о том, что на протяжении последних четырех лет сохраняются неизменно высокие показатели преступности в рассматриваемой сфере и низкий процент успешных расследований таких преступлений. Эти обстоятельства свидетельствуют о том, что разработанные ранее методики расследования преступлений оказываются недейственными в силу стремительного развития информационно-телекоммуникационных систем и технологий, которые стали катализатором в создании новых способов совершения преступлений. Рассматриваются выявленные автором проблемы, возникающие при расследовании преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий. Предлагаются практические рекомендации, оптимальные алгоритмы расследования таких преступлений.

Высокий уровень развития IT-технологий и их повсеместное распространение в информационном пространстве способствовали появлению новых способов совершения преступлений с использованием современных достижений научно-технического прогресса. Согласно статистическим данным в 2020 году правоохранительные органы Российской Федерации зарегистрировали 510400 преступлений, совершенных с помощью информационно-телекоммуникационных технологий. В 2021 году на деяния рассматриваемой категории пришлось каждое четвертое из зарегистрированных преступлений (517700 преступлений). В 2022 году было зарегистрировано 522100 преступлений, совершенных с помощью информационно-телекоммуникационных технологий[1] (см. иллюстрацию 1). Данные статистики свидетельствуют о постоянном росте количества преступлений, совершенных с помощью информационно-телекоммуникационных технологий, и относительно низком уровне их раскрываемости.

Проблемы расследования преступлений в современных условиях информационно-технологического развития общества рассматривались в работах таких ученых-криминалистов, как А.А. Бессонов, В.Б. Вехов, Е.П. Ищенко, П.С. Пастухов, Е.Р. Россинская и др.[2] Считаем правильным присоединиться к мнению В.В. Полякова, полагающего, что проблема низкой раскрываемости преступлений изучаемого нами вида вызваны неразработанностью частной криминалистической методики расследования высокотехнологич-

[1] Представлены сведения с Портала правовой статистики (Официальный сайт Генеральной прокуратуры Российской Федерации) // URL: http://crimestat.ru/analytics (дата обращения: 12.09.2023)).

[2] См., например: Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 3 (55). С. 46-52; Вехов В.Б., Пастухов П.С. Формирование стратегий расследования преступлений на основе положений электронной криминалистики // Ex jure. 2019. № 4. С. 129-141; Ищенко Е.П. У истоков цифровой криминалистики // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 3 (55). С. 15-28; Россинская Е.Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юридический вестник Самарского университета. 2019. № 4. С. 144-151.

ных преступлений [1, с. 85]. Перечень преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, весьма обширен, и прогнозы по дальнейшей информатизации общества позволяют говорить о том, что он будет все больше расширяться.

Необходимо иметь в виду, что у рассматриваемых преступлений есть специфические признаки:

- неочевидность, большая скрытность от человека и, как следствие, обнаружение пострадавшим следов преступления спустя большой промежуток времени с момента его фактического совершения;

- дистанционность, предполагающая значительное удаление местонахождения преступника от предмета преступного посягательства, не исключающая, в частности, их расположение на территориях разных государств. В последнем случае преступление носит транснациональный характер и подпадает под юрисдикцию разных государств. Согласно правовой позиции, сформулированной в п. 19 Постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»», местом совершения деяния в подобной ситуации следует признавать непосредственно ту территорию, на которой лицо физически находилось в момент использования тех или иных электронных устройств, в том числе переносных, для совершения преступлений указанного вида[1];

- высокотехнологичность, которая обусловливает возможности преступника почти мгновенно изменять значительные по объему информационные массивы, а также сложность обнаружения и фиксации цифровых следов преступления;

- трудность выявления и фиксации индивидуальной следовой информации, поскольку большинство преступлений совершается с многопользовательских рабочих мест и удаленных рабочих столов [2, с. 81].

Изучение материалов уголовных дел, возбужденных по фактам совершения преступлений рассматриваемого нами вида, позволило выявить ряд недостатков в расследовании таких преступлений:

1. Несвоевременное возбуждение уголовного дела влечет за собой невозможность раскрытия преступления по «горячим следам» и утрату доказательственной базы. Зачастую длительный срок предварительной проверки обусловлен отсутствием действенного инструментария, который позволял бы оперативно документировать цифровые

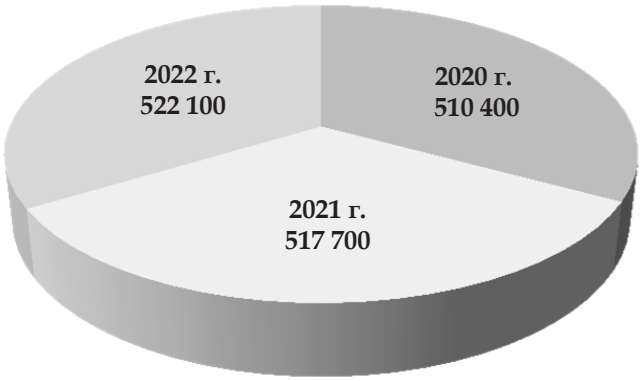

Иллюстрация 1. Статистические данные о преступлениях, совершенных с помощью информационно-телекоммуникационных технологий, за период с 2020 по 2022 г.

следы преступления: текстовые, аудио- и видеоданные, техническую информацию о месте, времени удаленного подключения, об использованном оборудовании, о взаимодействии пользователя с информационными системами и т.д. Для устранения правового пробела МВД России внесло на рассмотрение в Государственную думу Федерального собрания Российской Федерации законопроект, содержащий предложение о внесении изменения в п. 5 ч. 1 ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Предлагается в перечне оперативно-разыскных мероприятий вместо «исследование предметов и документов» использовать формулировку «исследование предметов, документов и информации, в том числе содержащейся в технологических системах ее передачи, включая информационно-телекоммуникационную сеть «Интернет»»[2].

2. Не в полной мере при расследовании хищений денежных средств с расчетных счетов кредитно-финансовых организаций используются возможности электронного документооборота. Следователи вместо направления соответствующих запросов в банки ограничиваются только документами, предоставленными потерпевшими.

3. Не осматриваются в качестве вещественных доказательств кассовые чеки, выписки о движении денежных средств по счетам, договоры на предоставление кредитных обязательств, а также иные предметы и документы, полученные в ходе расследования по уголовному делу, что также приводит к утрате криминалистически значимой информации[3].

Изложенное позволяет сделать вывод о необходимости дальнейшей разработки частной криминалистической методики расследования преступлений, совершенных с использованием современ-

[1] Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»».

[2] См.: Проект федерального закона от 14.08.2023 «О внесении изменения в статью 6 Федерального закона «Об оперативно-розыскной деятельности»» // Федеральный портал проектов нормативных правовых актов // URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=140881 (дата обращения: 28.09.2023).

[3] Обзор о результатах работы по профилактике, раскрытию и расследованию преступлений в сфере информационно-телекоммуникационных технологий в Волгоградской области за девять месяцев 2023 г. (на основании материалов уголовных дел) // Архив Главного управления МВД России по Волгоградской области.

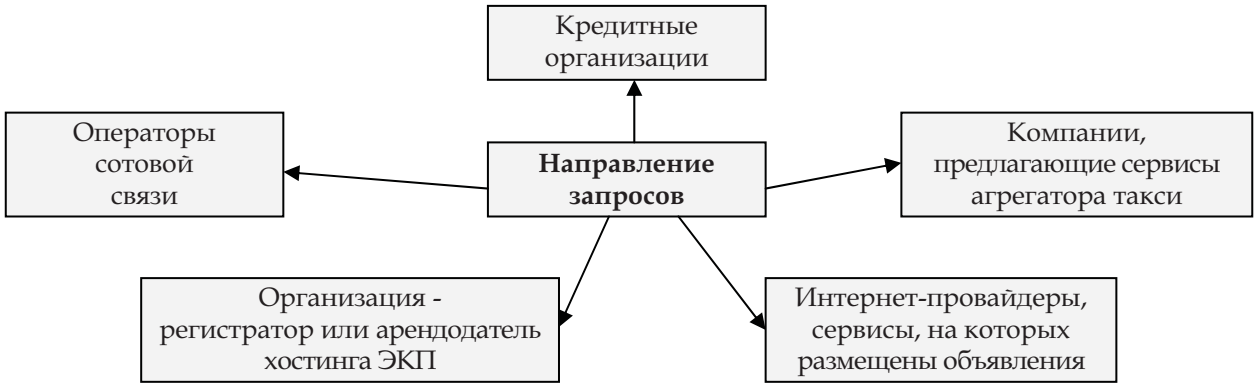

Иллюстрация 2. Схема направления запросов в организации.

ных информационно-телекоммуникационных технологий. В связи с этим следует определить перечень следственных, организационно-подготовительных и процессуальных действий, разработать научно обоснованные рекомендации по их наиболее оптимальному применению в целях достижения назначения уголовного судопроизводства.

В результате анализа материалов уголовных дел нами установлено, что при поступлении от граждан заявлений о совершении преступлений с использованием информационно-телекоммуникационных технологий в большинстве случаев следователями в дежурные сутки выполняется минимальный комплекс первоначальных следственных и процессуальных действий. Наукой и практикой для повышения эффективности расследования вырабатываются алгоритмы действий следователя. Рассмотрим оптимальную программу первоначального этапа расследования на примере хищений денежных средств с банковского счета потерпевшего путем мошенничества с использованием информационно-телекоммуникационных технологий.

Допрос потерпевшего. После вынесения постановления о признании потерпевшим лица, которому преступлением причинен ущерб, необходимо незамедлительно допросить его. В ходе допроса требуется выяснить следующие обстоятельства:

- обстановка совершения преступления: точное время, дата, место;

- способ совершения преступления; при телефонном мошенничестве выясняется абонентский номер, с которого поступил телефонный звонок, кем представился мошенник, предмет разговора со злоумышленником;

- подробное описание голоса преступника (хриплый, высокий, низкий, молодой или старый, наличие акцента, как говорил преступник, медленно или скороговоркой, иные особенности речи); у потерпевшего уточняется, сможет ли он опознать мошенника по голосу (в том числе при предъявлении аудиозаписи голоса), а также имеется ли у него аудиозапись разговора с мошенником (например, сделанной при помощи специальной программы в телефоне);

- номер расчетного счета или номер банковской карты, с использованием которой переведены похищенные денежные средства;

- использовались ли система быстрых переводов или терминалы кредитных организаций для внесения денежных средств на банковские счета для якобы их сохранения на безопасном счете;

- абонентские номера, на которые были зачислены денежные средства;

- сумма и размер причиненного ущерба, материальное положение потерпевшего.

А.Н. Литвиненко и М.А. Кирилюк справедливо отмечали, что каждый пользователь мобильной связи является потенциальным объектом атаки телефонных мошенников [3, с. 37]. В связи с этим в ходе допроса потерпевшего необходимо устанавливать его финансовое поведение (каковы размеры его доходов, ежедневных платежей, проводимых за оплату товаров, услуг, размеры кредитных обязательств и ежемесячных выплат по ним).

Выемка. При необходимости изъятия предметов и документов, имеющих значение для дела, целесообразно произвести выемку у потерпевшего мобильного телефона, на который поступил звонок, и документов, содержащих сведения о совершенном преступлении.

При описании изъятого мобильного телефона в протоколе обязательно указываются:

- индивидуальные признаки устройства (размер, цвет, материал, идентифицирующие признаки: царапины, сколы, потертости, трещины и их расположение);

- точное наименование устройства (марка, модель, год выпуска);

- IMEI-код мобильного телефона (следует установить, имеет ли это устройство несколько кодов IMEI);

- абонентский номер, который использовался в телефоне, на кого он зарегистрирован, какому мобильному оператору принадлежит, номер симкарты;

- наличие (или отсутствие) защитного пароля; если пароль имеется, то какой именно, используется ли ПИН-код, буквенно-цифровой пароль, графический ключ, Face ID, сканер отпечатка пальцев (по возможности следует отключить защиту).

При необходимости специалистом, участвующим в следственном действии, могут быть применены специализированные программные комплексы с использованием алгоритма искусственного интеллекта (например «Мобильный криминалист»). Использование программного комплекса позволяет извлечь информацию в полном объеме, даже с восстановлением удаленных файлов. Одновремен-

но устанавливаются графы взаимосвязей, геолокационные данные, временные метки.

Отдельно следует остановиться на порядке упаковки мобильных телефонов (смартфонов). Поскольку мобильный телефон является ценным источником криминалистически значимой информации, то его изъятие и упаковка требуют особого внимания. После осмотра на телефоне включается функция «авиарежим», чтобы исключить удаленный доступ к его содержимому.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами. Если устанавливается факт использования программ по подмене номера для производства звонков, то с целью установления лиц, совершивших преступление, необходимо получить протоколы соединений абонентского номера потерпевшего: посредством личного кабинета потерпевшего на сайте либо у оператора сотовой связи по постановлению суда. В последнем случае в суд направляется ходатайство о разрешении получения у оператора связи сведений о соединениях между абонентами и абонентскими устройствами. После получения информации можно установить абонентский номер, использованный мошенником для совершения звонка, а также дату, время, продолжительность соединения. Эта информация требуется для направления дальнейших запросов операторам связи.

Направленное в суд ходатайство о разрешении получения у оператора связи сведений о соединениях между абонентами и абонентскими устройствами по номерам телефонов, использованных мошенником для совершения преступления, должно также содержать запрос возможности получения у оператора связи информации об IMEI-кодах устройства, а также использованных с тем или иным IMEI-кодом сим-карт, о способах оплаты за услуги связи (номерах счетов, электронных кошельков, с которых она поступила).

Необходимо своевременно направить *запросы* в различные организации (иллюстрация 2).

В целях получения криминалистически значимой информации от учреждений финансово-кредитной системы, интернет-провайдеров, операторов сотовой связи и интернет-сервисов при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, должно быть организовано взаимодействие с различными коммерческими организациями посредством электронного документооборота. Так, в рамках взаимодействия, установленного в электронной форме, не позднее дня направления электронного запроса (в среднем - в течение 1 часа) ответы высылаются операторами сотовой связи АО «Мегафон» и ООО «Т2 Мобайл», учреждениями финансово-кредитной системы ПАО «Сбербанк», АО «Альфа-Банк», «QIWI банк», ПАО «ВТБ», ООО НКО «ЮМани» (Яндекс деньги). В запросе оператору сотовой связи, которому принадлежит номер телефона потерпевшего, целесообразно отразить необходимость предоставления информации о том, откуда поступил вызов (интернет-провайдер либо компания, предоставляющая услуги в сфере IP-телефонии). В запросе обязательно нужно указать номер телефона потерпевшего, номер телефона, с которого поступил звонок, дату, время и продолжительность телефонного соединения. После этого в установленную из полученного ответа организацию направляется запрос с просьбой предоставить регистрационные данные абонента, использовавшего номер телефона, с которого поступил звонок потерпевшему (указываются дата телефонного соединения, время, длительность разговора), данные о номере использованного оборудования, IP-адресе, шлюзе, номере trunk, об использованном программном обеспечении, виртуальной АТС, МГТС, направлении соединения, адресе интернет-ресурса. Можно запросить также сведения о способах оплаты за использование интернет-трафика. При получении ответа, в котором указана иная организация, направляется соответствующий запрос о получении аналогичных сведений. Запросы следует на-

KLIMOVA Y.A.,
PhD in Juridical Sciences,
Professor at the Criminalistics Department of the Educational and Scientific Complex for Preliminary Investigations in the Internal Affairs Bodies of the Volgograd Academy of the Ministry of the Interior of Russia

FEATURES OF THE METHODOLOGY FOR INVESTIGATING CRIMES COMMITTED USING MODERN INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Investigation of crimes, investigation methodology, information technologies, telecommunication technologies, IT technologies, Internet, digitalization, digital evidence.

The article analyzes statistical data on crimes committed using information and telecommunication technologies. It is concluded that over the past four years there have been consistently high crime rates in this area and a low percentage of successful investigations of such crimes. These circumstances indicate that previously developed methods for investigating crimes are ineffective due to the rapid development of information and telecommunication systems and technologies, which have become a catalyst in the creation of new methods of committing crimes. The problems identified by the author that arise during the investigation of crimes committed using modern information and communication technologies are considered. Practical recommendations and optimal algorithms for investigating such crimes are offered.

правлять до тех пор, пока не будет получен конечный ответ из организации, что при осуществлении указанных соединений использовались их оборудование, учетные записи и IP-адреса.

Факт использования подменного номера устанавливается при направлении запроса оператору связи, которому принадлежит абонентский номер, использованный мошенником. Необходимо запросить сведения о том, поступал ли с данного абонентского номера звонок потерпевшему в дату и время, когда ему звонил мошенник. В случае ответа оператора связи о том, что с указанного в запросе абонентского номера звонок потерпевшему не осуществлялся или номер телефона никому не выделялся, есть все основания полагать, что номер телефона мошенником был подменен.

При получении сведений об IP-адресе требуется направить запрос в компанию-провайдер, которой выделен данный адрес, для получения информации о лице, которому он предоставлен. При этом важно обязательно указать дату и время его использования, адресата (сайт или иной интернет-ресурс). Возможность установления принадлежности динамического IP-адреса (например оператора связи) зависит от точности указанного в запросе периода его использования мошенником (то есть необходимо обязательно указывать в запросе дату и время с точностью до секунд). Для определения провайдера IP-адреса следует проверить его по специальному Whois-сервису для идентификации доменов, что также позволяет установить организацию, которой принадлежит IP-адрес, и даже то, на какой хостинг-площадке размещается сайт[1].

Самыми популярными у мошенников сайтами являются «Avito.ru», «Юла», «Яндекс.Такси», а также социальные сети «ВКонтакте», «Instagram», мессенджеры «WhatsApp» и «Telegram». «Сбербанк-онлайн», «Qiwi Wallet» и ФК «Открытие» относятся к числу наиболее часто используемых для преступной деятельности приложений.

Использование подсистемы ИБД-Ф «Дистанционное мошенничество». Своевременное внесение в специализированную базу данных информации о возбуждении уголовного дела и сведений, полученных на первоначальном этапе расследования преступления, позволяет в кратчайшие сроки выявлять деяния, совершенные одними и теми же лицами, устанавливать их «серийность», что дает основание соединять в одном производстве уголовные дела, возбужденные в различных регионах Российской Федерации. Вместе с тем следует акцентировать внимание на тактических особенностях производства отдельных следственных действий, направленных на сбор и закрепление «цифровых» следов преступления, в том числе размещенных на электронных носителях информации, в сети Интернет (включая облачные хранилища), различных социальных сетях и т.п. Именно высокий уровень технологичности способа совершения преступлений предопределяет особенности производства отдельных следственных действий. Отметим, что данная характеристика указывает на необходимость повсеместного использования знаний специалистов, представляющих не только МВД России, но и иные организации и учреждения, в том числе негосударственные.

В заключение отметим, что применение на практике рассмотренных нами алгоритмов расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, будет способствовать повышению эффективности организации самого расследования и формированию необходимой для его производства методики. ■

Библиографический список:

1. Поляков В.В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений. // Lex russica (Русский закон). 2022. Т. 75. № 6 (187). С. 85-96.

2. Климова Я.А. Искусственный интеллект и цифровые доказательства в расследовании преступлений, совершенных с использованием современных информационно-коммуникационных технологий // Вестник Волгоградской академии МВД России. 2023. № 1 (64). С. 81-88.

3. Кирилюк М.А., Литвиненко А.Н. Методические подходы к исследованию дистанционных хищений денежных средств в Российской Федерации // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2023. № 3 (73). С. 35-42.

[1] Whois-сервис для проверки доменов // URL: http://www.whois-service.ru (дата обращения: 11.09.2023).