МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО РАБОТЕ С ЛИЧНЫМ СОСТАВОМ

ТАКТИКА ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Допущено Министерством внутренних дел Российской Федерации
в качестве учебного пособия для курсантов и слушателей
образовательных организаций системы МВД России,
сотрудников органов внутренних дел Российской Федерации

Москва
2025

УДК 343.9
ББК 67.629.4

Авторский коллектив:
Старичков М. В. – § 1 главы 1; § 4 главы 2;
Третьякова Е. И. – введение; § 1, § 2, § 3 главы 2; заключение;
Усачев С. И. – § 2 главы 1; § 5 главы 2

Тактика производства следственных действий при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий : учебное пособие / Е. И. Третьякова, М. В. Старичков, С. И. Усачев. – М. : ГУРЛС МВД России, 2025. – 128 с.

В учебном пособии на основе анализа криминалистически значимых сведений о преступлениях, совершенных с использованием ИТ-технологий, являющихся результатом обобщения следственно-судебной практики и научных исследований, представлены современные особенности использования указанных технологий в механизме преступной деятельности. Сформированы организационно-тактические аспекты проведения отдельных следственных действий при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Учебное пособие предназначено для курсантов и слушателей образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

УДК 343.9
ББК 67.629.4

Рецензенты:

Волгоградская академия МВД России:

кандидат юридических наук, доцент,
начальник кафедры предварительного расследования
учебно-научного комплекса по предварительному следствию
в органах внутренних дел **Бугера М. А.;**

кандидат технических наук, доцент,
доцент кафедры криминалистики учебно-научного комплекса
по предварительному следствию в органах внутренних дел **Курин А. А.;**

кандидат юридических наук, доцент,
доцент кафедры предварительного расследования
учебно-научного комплекса по предварительному следствию
в органах внутренних дел **Сафонова Ю.С.;**

Омская академия МВД России:

кандидат юридических наук, доцент,
начальник кафедры криминалистики **Горшков М. М. ;**

кандидат юридических наук, доцент,
заместитель начальника кафедры криминалистики **Соколов А. Б.;**

кандидат юридических наук, доцент,
доцент кафедры криминалистики **Анешева А. Т.;**

кандидат юридических наук, доцент,
доцент кафедры криминалистики **Неупокоева И. А.;**

Уральский юридический институт МВД России:

кандидат юридических наук,
заместитель начальника кафедры криминалистики **Дерюгин Р. А. ;**

кандидат юридических наук, доцент,
доцент кафедры криминалистики **Виноградова О. П.;**

старший преподаватель кафедры криминалистики **Мосин И. В. ;**

Уфимский юридический институт МВД России:

кандидат юридических наук, доцент,
начальник кафедры криминалистики **Нугаева Э. Д.;**

кандидат технических наук,
доцент кафедры криминалистики **Харисова З. И.;**

Следственный департамент МВД России:

кандидат юридических наук,
старший следователь по особо важным делам аналитического отдела
организационно-аналитического управления **Игнатова О Н.;**

Управление по борьбе с противоправным использованием
информационно-коммуникационных технологий МВД России:

оперуполномоченный по особо важным делам 2 отдела **Овсянников П. Н.;**

Экспертно-криминалистический центр МВД России:

доктор юридических наук, профессор, заместитель начальника управления научных
исследований – начальник отдела организации научных исследований
Гаврилин Ю. В.;

заместитель начальника отдела компьютерных и радиотехнических экспертиз
управления экспертиз цифровой и речевой информации **Савельев А. В.;**

учебно-методическая секция по учебным дисциплинам (модулям) в области
противодействия преступлениям, совершаемым с использованием
информационно-телекоммуникационных технологий, на базе
Московского университета МВД России имени В.Я. Кикотя.

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

МВД России – Министерство внутренних дел Российской Федерации.
Минюст России – Министерство юстиции Российской Федерации.
СК России – Следственный комитет Российской Федерации.
ФСБ России – Федеральная служба безопасности Российской Федерации.
ЭКЦ МВД России – Федеральное государственное казенное учреждение «Экспертно-криминалистический центр Министерства внутренних дел Российской Федерации».
ФКУ ГУФСИН России – Федеральное казенное учреждение Главного управления Федеральной службы исполнения наказаний Российской Федерации.
ГУНК МВД России – Главное управление по контролю за оборотом наркотиков Министерства внутренних дел Российской Федерации.
РЭО ГИБДД МВД России – Регистрационно-экзаменационное отделение Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации.
УК РФ – Уголовный кодекс Российской Федерации.
УПК РФ – Уголовно-процессуальный кодекс Российской Федерации.
ИТТ, ИТ-технологии – информационно-телекоммуникационные технологии.
QR-код – код быстрого отклика.
гр. – гражданин.
Госуслуги – Единый портал государственных услуг Российской Федерации.
МФЦ – многофункциональный центр предоставления государственных и муниципальных услуг.
НЖМД – накопитель на жестких магнитных дисках.
ПК – персональный компьютер.
полис ОСАГО – полис обязательного страхования автогражданской ответственности.
ПАО – публичное акционерное общество.
РТЭ – радиотехнической экспертизы.
мессенджеры – системы мгновенного обмена сообщениями.
СКТ – средства компьютерной техники.
ЭНИ – электронные носители информации.

СЛОВАРЬ ТЕРМИНОВ

Bluetooth – производственная спецификация беспроводных персональных сетей, обеспечивающая обмен информацией между различными устройствами (персональные компьютеры (настольные, карманные, ноутбуки), мобильные телефоны, интернет-планшеты, принтеры, цифровые фотоаппараты, мыши, клавиатуры, джойстики, наушники, гарнитуры и акустические системы) на надёжной, бесплатной, повсеместно доступной радиочастоте для ближней связи.

DHCP – это клиент-серверный протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol), с помощью которого в ИТ-инфраструктуре сетевые параметры каждого нового устройства прописываются автоматически.

DLP-система – специализированное программное обеспечение, предназначенное для защиты компании от утечек информации.

DNS-сервер – приложение, предназначенное для ответов на DNS-запросы по соответствующему протоколу.

GPS – спутниковая система навигации, обеспечивающая измерение расстояния, времени и определяющая местоположение во всемирной системе координат WGS 84.

IP-адрес (от англ. Internet Protocol Address) – сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

IP-телефония – голосовая связь, которая осуществляется по сетям передачи данных, в частности по IP-сетям (IP – Internet Protocol).

MacOS – операционная система компании Apple.

MAC-адрес (от англ. Media Access Control – управление доступом к среде) – уникальный идентификатор, сопоставляемый с различными типами оборудования для компьютерных сетей.

NFC – технология беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров.

RAM Scraper – вредоносная программа, которая сканирует основную память зараженных устройств для кражи конфиденциальных данных.

Spoofing (англ. spoofing – подмена) – ситуация, в которой один человек или программа успешно маскируется под другую путем фальсификации данных, что позволяет получить незаконные преимущества.

SSD – компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти, альтернатива жестким дискам (HDD).

TOR – система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания.

URL – адрес (от англ. Uniform Resource Locator – «единый указатель ресурса») – единообразный локатор (определитель местонахождения) ресурса.

USB Killer – модифицированный USB-накопитель, посылающий высоковольтное питание на компьютер, к которому он подключен, и тем самым эффективно разрушающий систему.

VPN (Виртуальная частная сеть) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) «поверх» другой сети.

Zombie – вредоносные программы для создания и внедрения на компьютер кода, который, подобно логической бомбе, будет активироваться при определенных условиях (обычно речь идет об удаленном доступе – отсылке команд). Впоследствии зомбированный компьютер используется для рассылки спама, проведения DDoS атак (распределенная атака в обслуживании), накрутки счетчиков и прочих вредоносных действий без ведома владельца.

Wi-Fi – технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11. Логотип Wi-Fi является торговой маркой Wi-Fi Alliance.

Авторизация – предоставление определенному лицу или группе лиц прав на выполнение определенных действий, а также процесс подтверждения данных прав при попытке выполнения этих действий.

Активатор – программа, позволяющая сгенерировать код, ключ, пароль и т. п. активации для другой компьютерной программы.

Анонимизация – совокупность действий, направленных на сокрытие личности пользователя путем маскировки или подмены характеристик пользователя и его устройств.

Антивирусное программное обеспечение – специализированное программное обеспечение для обнаружения нежелательных программ, восстановления измененных такими программами файлов, а также для предотвращения изменения такими программами файлов или операционной системы.

Аутентификация пользователя – процедура проверки подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных пользователей.

Аутентификация электронного письма – подтверждение подлинности электронного письма путем проверки цифровой подписи письма по открытому ключу отправителя.

Биткоин – первая самая популярная и самая распространенная криптовалюта в мире. Создана в 2009 году.

Блокчейн – выстроенная по определенным правилам непрерывная последовательная цепочка блоков, содержащих информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока. Изменение любой информации в блоке изменит его хеш-сумму.

Браузер – программа для поиска и просмотра информации из вычислительной сети.

Буфер обмена (англ. clipboard) – промежуточное хранилище данных, предоставляемое программным обеспечением и предназначенное для пере-

носа или копирования информации между приложениями или частями одного приложения через операции «вырезать», «копировать», «вставить».

Вирус – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Генератор ключей (кейген) (англ. Keygen) – небольшая программа, которая генерирует псевдоподлинные CD-ключи или серийные/регистрационные/активационные номера для регистрации/активирования ПО.

Дамп памяти – копия содержимого оперативной памяти, находящаяся на жестком диске или другом энергонезависимом устройстве памяти.

Деанонимизация – совокупность действий, совершаемых лицом или автоматизированной системой, направленных на раскрытие реальной личности пользователя и характеристик его устройств.

Домен – адрес веб-ресурса в сети Интернет.

Интернет-банкинг – общее название технологий дистанционного банковского обслуживания, а также доступ к счетам и операциям (по ним), предоставляющийся в любое время и с любого устройства, имеющего доступ в Интернет.

Интерфейс – совокупность возможностей одновременного совместного действия двух линейно не связанных систем либо системы и человека.

Кейлоггер – вредоносное программное или аппаратное устройство, предназначенное для скрытого мониторинга и записи нажатий клавиш.

Компаунд – термоактивная, термопластическая полимерная смола и эластомерные материалы с наполнителями и добавками или без них после затвердевания. Используется в качестве электроизоляционного материала и как средство взрывозащиты.

Логи-файл – текстовый файл, куда автоматически записывается важная информация о работе системы или программы сетевого оборудования.

Логическая бомба – специфический вид вредоносных программ, который проявляет себя только при определенных действиях или событиях (наступление дат, открытие каких-либо файлов и прочее), а остальную часть времени бездействует.

Метаданные файла – информация о другой информации, или данные, относящиеся к дополнительной информации о содержимом или объекте.

Оперативная память – энергозависимая часть системы компьютерной памяти, в которой во время работы компьютера хранится выполняемый машинный код (программы), а также входные, выходные и промежуточные данные, обрабатываемые процессором.

Оперативное запоминающее устройство – техническое устройство, реализующее функции оперативной памяти.

Операционная система – комплекс взаимосвязанных программ, предназначенных для управления ресурсами средств вычислительной техники и организации взаимодействия с пользователем.

Патчер – вспомогательная программа, автоматически обновляющая другую программу (например, до новой версии), либо исправляющая ошибки в старой версии, либо добавляющая новый функционал и т. п.

Регистратор доменного имени – организация, имеющая полномочия создавать (регистрировать) новые доменные имена и продлевать срок действия уже существующих доменных имен в домене, для которого установлена обязательная регистрация.

Руткит – набор вредоносных инструментов, представляющих несанкционированный доступ к программному обеспечению или всей операционной системе.

Свойства файла – атрибуты файла, определяемые операционной системой.

Сетевая карта (Ethernet-адаптер) – специальное интерфейсное устройство, которое позволяет компьютеру (ноутбуку) взаимодействовать с другими участниками локальной вычислительной сети.

Сетевой трафик (англ. traffic – «движение», «грузооборот») – объем информации, передаваемой через компьютерную сеть за определенный период времени.

Скриншот – мгновенный снимок экрана, осуществляемый нажатием клавиши «PrtScr» на клавиатуре.

Средства компьютерной техники – совокупность технических устройств, способных функционировать самостоятельно или в составе других систем, и программ, обеспечивающих их функционирование.

Социальная инженерия – метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании человеческих слабостей и считается очень разрушительным.

Троянская программа – программа, не обладающая возможностью самораспространения, маскирующаяся под легитимный файл.

Учетная запись – совокупность данных о пользователе, необходимая для его аутентификации и предоставления доступа к его личным данным и настройкам.

Файл – поименованный набор данных, расположенный на машинном носителе информации.

Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

Хостинговая компания – организация, оказывающая услуги по предоставлению вычислительных мощностей для размещения информации на сервере, постоянно находящемся в сети Интернет.

Червь – программа, обладающая способностью к самораспространению в компьютерных сетях через сетевые ресурсы.

Электронная почта – корреспонденция в виде сообщений, передаваемая между пользователями через вычислительную сеть.

ВВЕДЕНИЕ

Современная цивилизация характеризуется стремительным развитием высоких технологий, которые прочно вошли в жизнь человека, общества и государства. Широкий спектр использования, безграничные возможности и доступность цифровых технологий и цифровых инструментов значительно расширяют возможности человека, приводя к повышению эффективности взаимодействия субъектов в различных видах деятельности. Повсеместная цифровизация общества способствует революционным изменениям в технологической и экономической отраслях. В этой связи приоритетным направлением является развитие цифровой экономики, совершенствование информационно-телекоммуникационных технологий, внедрение их в сферы государственного управления и бизнеса. Указом Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»[1] определены основные принципы такого развития, которые сводятся прежде всего к обеспечению доступности информации для граждан и обеспечению защиты их интересов в информационной среде.

Однако в современной действительности «информация», в том числе и компьютерная, имея особое значение для человека, нередко становится объектом, предметом, а также средством совершения преступления. Ее распространенность, доступность и ценность определяют возникновение повышенного интереса к ней, и в то же время низкий уровень системы защиты делает ее уязвимой перед противоправным воздействием.

Кроме того, в настоящее время помимо преступлений в сфере компьютерной информации (глава 28 УК РФ[2]) информационные технологии начинают активно внедряться в механизм других, «традиционных», преступлений, в которых компьютерная информация становится отображением преступной деятельности – цифровым следом.

В этой части уголовное законодательство Российской Федерации, реагируя на происходящие изменения в структуре современной преступности, изменяется и в некоторые уголовно-правовые нормы, включены новые квалифицирующие признаки, характеризующие преступление как

---

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Официальный интернет-портал правовой информации : сайт. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687.

[2] Уголовный кодекс Российской Федерации : УК : принят Гос. Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/.

совершенное с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет).

Уголовно-процессуальное законодательство Российской Федерации, признавая ЭНИ и их содержание доказательством, пытается выработать порядок закрепления цифровой информации в качестве доказательств.

Очевидно, что криминалистическая наука, являясь интегративной и практико-ориентированной, должна обеспечивать современные потребности деятельности правоприменителей по раскрытию и расследованию преступлений, совершенных с использованием ИТТ. Большой вклад в развитие теории информационно-компьютерного обеспечения криминалистической деятельности внесли Багмет А. М., Васюков В. Ф., Вехов В. Б., Гаврилин Ю. В., Ищенко Е. П., Мещеряков В. А., Осипенко А. Л., Россинская Е. Р., Смушкин А. Б., Яковлев А. Н. и ряд других ученых. Выработанные учения о способах компьютерных преступлений (правонарушений), о цифровых следах как источниках криминалистически значимой компьютерной информации, о криминалистическом исследовании компьютерных средств и систем, входящие в структуру разрабатываемой теории, прошли «фильтр» жестких требований при формировании и признании, а практическая востребованность выработанных учений и теорий со временем только вырастет.

Анализ статистических данных позволяет определить наметившуюся устойчивую тенденцию ежегодного увеличения количества преступлений, совершенных с использованием ИТТ, и вряд ли в ближайшем будущем она изменится. Так, в 2019 г. зарегистрировано 294 409 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что составило 14,5 % от всей зарегистрированной преступности, в 2020 г. количество таких преступлений возросло до 510 396 и составило 24,9 %, в 2021 г. – 517 722 преступлений (25,8 % от общего числа), в 2022 г. – 522 065 преступлений (27,27 % от общего количества зарегистрированных преступлений), в 2023 г. их количество достигло 676 951 преступлений, что составило 34,7% от общего числа зарегистрированных преступлений; в 2024 г. – 765 365 преступлений, что составило уже 40% от общего числа зарегистрированных преступлений. В то же время следует отметить очень низкий уровень раскрываемости рассматриваемых преступлений. В 2019 г. раскрываемость составила 22,1 % – 65 238 преступлений, в 2020 г. – 18,6 % (94 942 преступления), в 2021 г. раскрыто 22,9 % (118 920 преступлений), в 2022 г. – 26,5 % (142 384 преступления), в 2023 г. – 25,5 % (172 290 преступлений), в 2024 г. раскрываемость составила 22,5 % (172 627 преступлений)[1].

---

[1] Статистика и аналитика // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/.

Низкий процент раскрываемости преступлений, совершенных с использованием ИТТ, связан преимущественно с особенностью способа их совершения и, соответственно, механизма следообразования. Наибольший процент таких преступлений совершается с использованием сети Интернет –84,8 %; 45,2 % преступлений – с использованием средств мобильной связи, 15 % – с использованием расчетных пластиковых карт, и с помощью компьютерной техники – 5,5 %[1]. А нередко при совершении рассматриваемых преступлений используется вся совокупность указанных технологий. Поэтому сегодня структура таких преступлений качественно меняется, и способы их совершения становятся все сложнее, что обусловлено бурным развитием информационных технологий, большим разнообразием компьютерных устройств, имеющих множество функциональных возможностей и позволяющих анонимизировать данные личности в цифровом пространстве, их доступностью и распространенностью.

Именно сеть Интернет, информационные технологии и средства сохраняют в памяти отражение преступного события в виде цифровых следов. Специфичность образования и материального воспроизведения, уязвимость и сложность их выявления, а также потребности следственной практики определяют необходимость выработки эффективного информационно-технологического инструментария для работы с цифровыми следами в ходе следственных действий, рекомендации по проведению которых служат основой для совершенствования частных методик расследования отдельных видов преступлений.

В учебном пособии на основе правоприменительной практики рассмотрены тактические приемы по производству осмотра отдельных объектов в зависимости от сложившейся следственной ситуации, допроса различных участников уголовного судопроизводства, обыска, выемки; получению информации о соединениях между абонентами и (или) абонентскими устройствами, а также назначению судебных экспертиз. Рассмотренные следственные действия являются наиболее значимыми в системе доказательств по преступлениям, совершенных с использованием ИТТ.

В целях закрепления и проверки уровня освоения теоретического материала в конце каждого параграфа даны контрольные вопросы. В приложении к пособию предложены тестовые и практические задания, позволяющие сформировать умения и навыки по тактике производства отдельных следственных действий, направленных на получение доказательств и криминалистически значимой информации при расследовании преступлений, совершенных с использованием ИТТ.

---

[1] Статистика и аналитика // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Криминалистически значимые свойства преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Современная цивилизация немыслима без информационно-телекоммуникационных технологий. Информация становится одним из основных ресурсов. Недаром XXI век уже называют «информационным». Соответственно, и при совершении противоправных деяний все чаще используются информационно-телекоммуникационные технологии. В настоящее время можно выделить четыре группы таких преступлений:

1. «Компьютерные преступления», к которым относятся преступления в сфере компьютерной информации (гл. 28 УК РФ), а также некоторые преступления, совершение которых возможно только с использованием ИТТ, например кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ).

2. Преступления, совершаемые с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет), например, предусмотренные п. «д» ч. 2 ст. 110 УК РФ, п. «в» ч. 3 и п. «в» ч. 5 ст. 222 УК РФ, п. «б» ч. 2 ст. 222.1 УК РФ, п. «б» ч. 3 ст. 242 УК РФ, ч. 2 ст. 280 УК РФ. Использование ИТТ является для них неотъемлемым элементом способа совершения преступления.

3. «Традиционные» преступления, способ совершения которых связан с использованием ИТТ, что определяет особенности следообразования, например дистанционное мошенничество.

4. Иные преступления, при подготовке, совершении и (или) сокрытии которых в качестве вспомогательного средства использовались ИТТ, а также для которых электронные носители информации выступают как носители криминалистически значимой информации (например, служат средством коммуникации или содержат характеризующие личность преступника сведения).

Комплекс криминалистически значимых сведений о преступлении, являющийся результатом обобщения следственно-судебной практики и научных исследований, составляет криминалистическую характеристику, обычно рассматриваемую как элемент частной методики расследования отдельных видов и групп преступления.

В рамках криминалистической тактики не принято анализировать криминалистическую характеристику преступления. Однако преступления, совершенные с использованием информационно-телекоммуникационных технологий, обладают рядом специфических свойств, не всегда понятных и очевидных на обыденном уровне. Понимание этих свойств позволит лицу, производящему расследование, эффективно и грамотно как с процессуальной, так и с технической точки зрения выявлять, фиксировать, изымать и использовать в процессе доказывания криминалистически значимую информацию о таких преступлениях.

В качестве основных структурных элементов преступлений, совершенных с использованием ИТТ, можно выделить следующие криминалистически значимые сведения:

– о предмете преступного посягательства и личности потерпевшего (пострадавшей стороны);

– о личности преступника, мотивах и целях его преступного поведения;

– об обстановке преступных посягательств, включающей время и место;

– о способе совершения преступления, включая его подготовку и сокрытие, а также посткриминальное поведение преступника;

– о механизме следообразования;

– об обстоятельствах, способствовавших совершению преступления.

Понятие предмета посягательства в преступлениях, совершенных с использованием ИТТ, достаточно широкое и зависит от того, в какой сфере совершается данное преступление, то есть в соответствии с какой статьей УК РФ оно квалифицируется.

Большинство таких преступлений носит корыстный характер, соответственно, предметом преступления чаще всего выступают деньги и иные материальные ценности, либо связанные с ними имущественные права, реже – иные материальные блага (например, возможность безвозмездно пользоваться платным контентом). Характерной особенностью является то, что воздействие осуществляется не непосредственно на предмет (как в ходе «обычной» кражи), а на его «информационную составляющую» – сведения о самом предмете (права на денежные средства, движимое и недвижимое имущество), представление других лиц о предмете (понуждение собственника путем обмана или злоупотребления доверием к передаче имущества преступнику), использование информации для ведения недобросовестной конкуренции (тем самым осуществляется необоснованное обогащение) и т. п. Таким образом, фактически осуществляется

воздействие на информационные ресурсы. В некорыстных информационных преступлениях такое воздействие становится более очевидным.

В соответствии с ч. 1 ст. 42 УПК РФ[1], потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо – в случае причинения преступлением вреда его имуществу и деловой репутации. Потерпевший – это процессуальный статус, который возникает у лица после возбуждения уголовного дела и принятия решения о признании его таковым. Однако вред преступлением может быть причинен другим лицам, и не только прямой, но и косвенный. Например, в результате неправомерных действий в информационно-телекоммуникационной сфере произошел рейдерский захват и банкротство предприятия. Оставшиеся безработными люди с точки зрения закона потерпевшими признаны не будут, хотя их интересам, бесспорно, причинен вред. Поэтому, говоря об информационно-телекоммуникационных, целесообразно использовать понятие «пострадавшая сторона», объединяющее как участников уголовного процесса: потерпевшего, гражданского истца, частного обвинителя (например, по уголовным делам о клевете, содержащейся в распространяемом с использованием информационно-телекоммуникационных сетей сообщении, – ст. 128.1 УК РФ), их представителей, так и иных лиц, чьи права и законные интересы были нарушены.

Поскольку у собственности всегда существует собственник, он и будет являться потерпевшим. Если же преступление направлено на причинение вреда информационным ресурсам, можно выделить следующие категории потерпевших (пострадавшей стороны):

– собственники (владельцы) информационных ресурсов;

– собственники (владельцы) средств компьютерной техники, на которых хранятся информационные ресурсы, а также собственники (владельцы) информационно-телекоммуникационных систем, предоставляющих услуги доступа к информационным ресурсам;

– лица, сведения о которых хранятся (обрабатываются) в информационных системах и образуют информационные ресурсы;

– лица, пользующиеся информационными ресурсами, средствами компьютерной техники и информационно-телекоммуникационными системами;

– прочие лица, правам и законным интересам которых в результате неправомерного поведения в информационно-телекоммуникационной среде причинен вред.

---

[1] Уголовно-процессуальный кодекс Российской Федерации : УПК : принят Гос. Думой 22 ноября 2001 г. : одобрен Советом Федерации 5 декабря 2001 г. : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/.

Можно говорить о достаточно высокой виктимности поведения потерпевших[1]. Так, использование преступниками различных способов психологического воздействия нередко побуждает потерпевших передать им свои персональные данные, в том числе сведения для доступа к банковским счетам. В дальнейшем потерпевший может осознать, что сам способствовал совершению преступления, и это определяет особенности его поведения в ходе расследования уголовного дела, в частности вызывает умалчивание о подробностях своих действий. Возможность разглашения сведений интимного характера либо своего противоправного поведения (попытки дачи взятки должностному лицу, уклонения от уплаты налогов и сборов, распространения запрещенных или ограниченных в обороте предметов и др.) также побуждает потерпевших скрывать часть информации от следствия. Степень осведомленности потерпевшего о порядке функционирования информационных технологий разная, но в подавляющем большинстве это люди, обладающие лишь элементарными навыками работы на компьютерных устройствах, позволяющими использовать информационные технологии в повседневной жизни (производство платежей, запись в государственные учреждения, покупка товаров через Интернет и т. п.).

Важным компонентом, характеризующим преступления, совершенные с использованием ИТТ, являются сведения об особенностях личности преступника. Характеристики личности такого преступника очень сильно варьируются в зависимости от вида совершаемого преступления. Например, совершение преступления, сопряженного с неправомерным доступом к компьютерной информации, в большинстве случаев требует от преступника хороших знаний в области ИТТ. В то же время для телефонного мошенничества зачастую достаточно владения основами межличностной коммуникации, как правило, на интуитивном уровне, что ставит такого преступника в один ряд с «традиционным» мошенником[2].

Характерные мотивы и цели преступлений, совершенных с использованием ИТТ, следующие:

---

[1] Касаев И. Х., Богомолова К. И., Лиходаев Е. Г., Грачева О. А. Виктимологическая характеристика преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Вестник Российского университета кооперации. 2022. № 4 (50). С. 95–96.

[2] О личности преступника, совершающего преступления с использованием ИТТ, см. например: Ищук Я. Г., Пинкевич Е. С., Аксенов В. А., Молчанова Т. В. Цифровая криминология. М. : Академия управления МВД России, 2021. 244 с.; Аксенов В. А. Особенности личности современного интернет-мошенника в механизме индивидуального преступного поведения // Криминологический журнал. 2020. № 4. С. 79–86.

– корыстные соображения: незаконное получение денег, ценных бумаг, кредита, материальных ценностей, товаров, услуг, привилегий, льгот, квот, недвижимости; уклонение от уплаты налогов, платежей, сборов и т. п.; легализация (отмывание) преступных доходов; получение конфиденциальной информации в корыстных целях (шантаж, игра на бирже, заключение выгодных сделок) и т. п.;

– политические цели: терроризм, шпионаж, акции, направленные на подрыв финансово-экономической стабильности государства, разжигание расовой, национальной, религиозной ненависти и т. п.;

– исследовательский интерес и любопытство;

– хулиганские побуждения и озорство;

– месть (конкретным лицам, организациям или «всему человечеству») – может являться следствием психического заболевания;

– стремление к самоутверждению, желание получить известность, приобрести авторитет в своем кругу, продемонстрировать свое интеллектуальное превосходство;

– намерение скрыть другое преступление или облегчить его совершение.

Предмет преступного посягательства нередко указывает на определенную категорию преступников. Например, секреты производства могут представлять интерес для конкурентов, клеветническая информация о политическом деятеле в сети Интернет распространяется в интересах его оппонентов.

Обстановка совершения преступления с использованием ИТТ включает взаимодействующие между собой до и в момент преступления материальные и социально-психологические факторы среды, в которой происходит преступное деяние. Она во многом определяет особенности поведения преступника и пострадавшей стороны, оказывает влияние на формирование остальных характеристик преступления рассматриваемой категории.

На обстановку подготовки, совершения и сокрытия таких преступлений значительное влияние оказывают условия деятельности пострадавшей стороны. Среди них можно выделить следующие факторы:

– вид деятельности или род занятия (сфера деятельности – управленческая, коммерческая, финансовая, производственная, информационная и т. д.);

– форма собственности и организационная структура юридического лица или правовой статус физического лица, правовой режим отдельных видов имущества, в т. ч. информации и информационных ресурсов;

– сфера деятельности, характер производимых и потребляемых ресурсов, в т. ч. интеллектуальных;

– кадровое и материально-техническое обеспечение, наличие необходимых помещений и оборудования;

– вид используемых СКТ, связи и телекоммуникаций, их технические характеристики и конструктивные особенности;

– организация движения товарно-материальных ценностей;

– организация документооборота и информационного обмена;

– система учета и отчетности;

– наличие и техническое состояние охраны, средств защиты информации и т. д.

К факторам деятельности пострадавшей стороны, формирующим обстановку, способствующую совершению преступлений с использованием ИТТ, относятся следующие:

– несовершенство средств защиты информации или полное их отсутствие;

– нарушение правил работы с охраняемой законом информацией, пренебрежение правилами защиты информации, отсутствие контроля над утилизацией (уничтожением) отходов информационного оборота;

– использование средств компьютерной и информационно-телекоммуникационной техники для обработки посторонней информации, в т. ч. в личных целях;

– неблагоприятный психологический климат в коллективе, конфликты между сотрудниками, неудовлетворенность отдельных работников своими руководителями или условиями труда.

Время совершения преступлений с использованием ИТТ не всегда устанавливается с точностью до дня и тем более – до часов и минут. Обычно это удается, когда момент подключения / отключения фиксируется на сервере тарификации оператора, предоставляющего услуги связи, в протоколах соединений, в системных журналах и т. п. Нередко время совершения данных преступных деяний, особенно многоэпизодных, определяется различными по продолжительности периодами, связанными с противоправной деятельностью. Следует помнить, что в соответствии с ч. 2 ст. 9 УК РФ временем совершения преступления признается время совершения общественно опасного деяния, независимо от времени наступления последствий. Вместе с тем моментом окончания преступления, совершенного с использованием ИТТ, является момент наступления указанных в диспозиции соответствующей статьи УК РФ общественно опасных последствий.

Отличительным свойством преступлений с использованием ИТТ является то, что общественно опасные действия могут совершаться в одном месте, а вредоносные последствия наступать в другом, часто находящемся на значительном расстоянии. При этом лицо не вступает в непосредственный контакт с информационной системой пострадавшей стороны. В связи с этим под местом совершения такого преступления понимается место, где было совершено общественно опасное деяние,

то есть где находилось информационно-телекоммуникационное оборудование, которым воспользовался преступник (п. 19 постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37[1]). Данным принципом руководствуются при определении территориальной подследственности в соответствии со ст. 152 УПК РФ.

В отличие от места совершения преступления, место происшествия характеризуется наличием следовой картины, оставленной в результате преступления. Для данной категории преступлений выделяют:

– место, где производились преступные деяния (осуществлялся доступ к компьютерной сети, вводились команды и информация, создавались вредоносные компьютерные программы и т. п.);

– место, где хранилась компьютерная информация, противоправное воздействие на которую причинило вред;

– место, где наступили общественно опасные последствия;

– иные места (место расположения транзитных носителей и др.).

Перечисленные места могут совпадать в любой комбинации, но могут и различаться. Следовательно, мест происшествия для преступлений, совершенных с использованием ИТТ, может быть несколько, в том числе значительно удаленных друг от друга и расположенных не только в разных помещениях, но и в разных населенных пунктах, и даже за рубежом.

Важнейшим и определяющим элементом, характеризующим любое, в том числе и совершенное с использованием ИТТ, преступление, является совокупность данных о способе его совершения. Способы совершения преступлений с использованием ИТТ отличаются большим разнообразием, что отмечалось в начале настоящего параграфа[2]. Кроме того, структура преступлений, совершенных с использованием ИТТ, достаточно быстро изменяется во времени. Например, если в начале 2000-х годов почти половина зарегистрированных преступлений в сфере компьютерной информации приходилась на подключение к информационно-телекоммуникационной сети Интернет под чужими регистрационными именами и паролями, то сейчас такие деяния редки. Зато почти не встречавшиеся тогда кражи с банковских счетов граждан (ввиду низкой распространен-

---

[1] 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» : постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/.

[2] Более подробно о способах совершения преступлений с использованием ИТТ см. § 2 настоящей главы («Информационно-телекоммуникационные технологии в механизме преступной деятельности»).

ности платежных карт среди населения) с появлением смартфонов, позволяющих подключить услугу «мобильный банк», становятся одним из самых частых информационно-телекоммуникационных преступлений. По-прежнему высокую опасность представляют хищения и злоупотребления путем модификации компьютерной информации лицами, имеющими доступ к компьютерной информации в силу своего служебного положения, а также создаваемые и распространяемые по информационно-телекоммуникационным сетям вредоносные компьютерные программы, особенно вирусного типа. Незаконное распространение запрещенных и ограниченных в обороте предметов (наркотических средств и психотропных веществ, оружия, порнографических материалов и т. д.) в настоящее время также осуществляется в основном с использованием информационно-телекоммуникационных сетей.

Грамотное производство следственных действий невозможно без понимания следователем механизма следообразования. В настоящее время преступления, сопряженные с использованием информационно-телекоммуникационных средств, характеризуются следующей следовой картиной:

– следы на средствах ИТ-техники и оборудования, с помощью которых лицо совершало преступление (следы на орудии преступления): использовавшееся для неправомерного доступа программное обеспечение, протоколы подключения к информационно-телекоммуникационным сетям, сохраненные коды доступа, тексты программ, скопированная у пострадавшей стороны информация и т. п. Такие следы могут остаться в операционной системе, в аппаратно-программной конфигурации, на электронных носителях;

– следы на «транзитных» (телекоммуникационных) носителях информации, посредством которых лицо осуществляло связь с охраняемыми законом информационными ресурсами: документированная информация о трафике через оператора телематических услуг, размещенная в сети информация, электронная переписка и т. д.;

– следы в подвергшейся вредоносному воздействию информационно-телекоммуникационной системе, в т. ч. на электронных носителях (следы на предмете преступления): результаты уничтожения, блокирования, модификации, копирования компьютерной информации, нейтрализации средств защиты компьютерной информации; протоколы соединений абонентов и др. Их местонахождение сходно со следами в ИТ-системе нарушителя (следами на орудии преступления);

– следы на ином ИТ-оборудовании, непосредственно не участвовавшем в совершении преступления, но содержащем имеющие значение для уголовного дела сведения, – криминалистически значимая информация в компьютерах, органайзерах, мобильных телефонах, цифровых фотоаппаратах, видеокамерах и диктофонах, смарт-картах и т. д.;

– документы, изготовленные с использованием средств компьютерной техники;

– документы, предназначенные для обработки в автоматизированных информационных системах, и иные документы, отражающие преступную деятельность;

– традиционные следы – рук, обуви, орудий, инструментов и т. д.;

– идеальные следы – сведения о преступлении и об относящихся к нему обстоятельствах, сохранившиеся в памяти участников преступления (преступников, потерпевших) и очевидцев, а также иных лиц.

Первые четыре пункта образуют так называемые «цифровые следы» («электронные следы», «виртуальные следы», «компьютерные следы»), учение о которых уже сформировано в теории криминалистики, – зафиксированные на электронных носителях информации (машинных носителях) криминалистически значимые сведения о преступлении.

Необходимо отметить, что информационная компьютерная система, в частности основа ее управления – операционная система, одновременно выступает и как следообразующий, и как следовоспринимающий объект. Поэтому неосторожное, неумелое обращение с ней может привести к безвозвратной утрате криминалистически значимой информации.

Уяснение и правильное толкование следовой картины имеет чрезвычайно важное значение для формирования методических основ расследования преступлений, совершенных с использованием ИТТ, поскольку определяет сущность всех исходных данных для организации и проведения следственных действий.

Среди основных обстоятельств, способствующих совершению преступлений с использованием ИТТ, следует отметить пренебрежение пострадавшей стороной мерами информационной безопасности. Другой фактор, существенно облегчающий преступникам анонимизацию в информационно-телекоммуникационных сетях, – продажа / покупка сим-карт мобильной связи без регистрации в нарушение установленных правил. Недостаточный контроль распространения запрещенной (ограниченной к распространению) информации в сети Интернет и возможность использования «теневого Интернета» также способствуют совершению преступлений рассматриваемой категории.

Кроме того, конкретные информационные ресурсы представляют для преступников (их определенных групп) повышенный интерес. Попытки противоправного воздействия в зависимости от ценности информации для злоумышленника могут предприниматься даже при наличии очень надежной защиты. Вид информации зависит от цели и мотивов преступника. Это могут быть сведения, составляющие охраняемую законом тайну (особенно государственную), представляющие повышенную материальную ценность (коммерческая тайна – секреты производства, «ноу-хау», инсайдерская информация, банковская тайна – номера кре-

дитных и расчетных карт, объекты авторского права – программное обеспечение, аудиовизуальная продукция и т. п.), информация о «публичных лицах» (персональные данные политиков, артистов и др.), сайты органов государственной власти, политических и общественных организаций, крупнейших компаний и т. д.

Контрольные вопросы

1. Какие группы преступлений, совершенных с использованием информационно-телекоммуникационных технологий, можно выделить? Дайте их краткую характеристику.
2. Назовите группы криминалистически значимых сведений, характеризующих преступления, совершенные с использованием ИТ-технологий. Какое значение они имеют для тактики производства следственных действий?
3. Охарактеризуйте личность преступника, совершающего преступления с использованием ИТ-технологий.
4. Какие следы образуются в результате преступлений, совершенных с использованием ИТТ?
5. Перечислите обстоятельства, способствующие совершению преступлений с использованием информационно-телекоммуникационных технологий.

§ 2. Информационно-телекоммуникационные технологии в механизме преступной деятельности

ИТТ в последние годы набирают стремительную популярность. Этому способствует ряд причин:

– развитие технологий (рост вычислительных мощностей компьютерной техники и смартфонов, совершенствование стандартов мобильной связи: внедрение сетей пятого поколения 5G[1], использование волоконно-оптической связи провайдерами, технологий искусственного интеллекта, машинного обучения, интернета вещей и т. д.);

– повышение уровня вовлеченности граждан в использование современных технологий и различных платформ (необходимость оплаты услуг посредством «интернет-банкинга», использование Госуслуг, создание в крупных компаниях различных виртуальных помощников, голосовых ассистентов, чат-ботов, с которыми приходится взаимодей-

[1] Правительственная комиссия одобрила дорожную карту развития 5G в России // ООО «МИЦ «Известия» : сайт. URL: https://iz.ru/1089281/2020-11-19 pravitelstvennaia-komissiia-odobrila-dorozhnuiu-kartu-razvitiia-5g-v-rossii.

ствовать потребителям каких-либо услуг). Отметим, что такое вовлечение нередко происходит от «безальтернативности». Например, запись в отделения РЭО, МФЦ просто невозможна традиционными способами (по телефону, либо личный визит) – на сегодняшний день подобные действия зачастую совершаются только через личные кабинеты либо через «Госуслуги».

Однако, несмотря на повсеместность использования современных ИТ-технологий во всех сферах жизни, уровень знаний граждан об их функциональных возможностях, системе обеспечения информационной безопасности и приватности остается низким. В связи с этим выбор преступников между использованием информационных технологий в качестве основного или вспомогательного средства при совершении различных преступлений и традиционным способом преступления очевиден. Вопрос масштабной «информационной безграмотности» настолько актуален, что существуют предложения о создании должности уполномоченного по защите прав человека в сфере информационно-телекоммуникационных технологий, который мог бы оказать содействие гражданам в восстановлении их прав и законных интересов, которые были нарушены или не соблюдены в информационном пространстве[1].

Небезопасное использование ИТТ в повседневной жизни делает уязвимой информацию о жизнедеятельности человека, в первую очередь информацию о персональных данных, финансовом положении, которая может быть использована в преступных целях. К тому же, как отмечалось ранее, стремительное развитие информационных технологий отражается на способе реализации преступного умысла и, как следствие, на механизме преступления. Поэтому можно уверенно говорить о влиянии развития информационных технологий на трансформацию преступлений. Появление новаций в цифровой среде закономерно влечет появление новых способов совершения преступлений[2].

Васильев А. Н. одним из первых ученых-криминалистов сформулировал само понятие «механизм преступления», которое раскрывалось как «процесс совершения преступления, в том числе его способ, и все действия преступника, сопровождающиеся образованием следов материаль-

---

[1] Мочалов А. Н. Об учреждении в России должности уполномоченного по защите прав человека в сфере информационно-телекоммуникационных технологий // Правовое государство: теория и практика. 2022. № 2 (68). С. 27–39.

[2] Рудых А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : дис. … канд. юрид. наук / Ростовский юридический институт МВД России. Ростов н/Д, 2020. 239 с.

ных и нематериальных, могущих быть использованными для раскрытия и расследования преступления»[1].

Исследование закономерностей возникновения и формирования криминалистически значимой информации рассматриваемых преступлений необходимо через понятие механизма преступления, который представляет собой сложную динамическую систему, определяющую содержание преступной деятельности[2]. Элементами механизма преступления являются: субъекты преступления; отношение субъекта преступления к своим действиям, их последствиям, соучастникам; предмет посягательства; способ преступления; преступный результат; обстановка преступления (место, время и другие относящиеся к ней обстоятельства); поведение и действия лиц, оказавшихся случайными участниками события, и т. п.[3]

Таким образом, криминалистическое учение о механизме преступления позволяет комплексно исследовать преступную деятельность.

Центральным звеном механизма преступления, в котором отражается факт использования информационных технологий, является способ совершения преступления, который в свою очередь обусловливает формирование иных специфичных элементов механизма, таких как механизм следообразования, средство совершения преступления и иные.

Умение ориентироваться в разнообразии ИТТ, особенностях их работы, навык определения слабых, уязвимых сторон позволят в дальнейшем анализировать возникающие следственные ситуации, выдвигать актуальные версии и использовать весь потенциал правоохранительной системы для успешного выявления, расследования и предупреждения преступлений, совершаемых с использованием ИТТ.

Мобильные телефоны, персональные компьютеры, ноутбуки, планшеты и другие компьютерные устройства, использующие электронную или информационно-телекоммуникационную сети, являются основными средствами совершения преступлений в сфере ИТТ. Следует отметить, что понятия электронной и информационно-телекоммуникационной сетей не разграничиваются, в соответствии с постановлением 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 ин-

---

[1] Криминалистика : учебник / Б. Е. Богданов, А. Н. Васильев, В. Я. Колдин и др.; отв. ред. А. Н. Васильев. М. : Изд-во Моск. ун-та, 1971. С. 7–8.

[2] Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская и др. М., 2023. С. 15.

[3] Россинская Е. Р. Криминалистика : учебник для вузов. М. : Норма-ИНФРА-М, 2016. С. 17.

формационно-телекоммуникационных сетей, включая сеть «Интернет», и сеть Интернет является одной из них, представляя собой технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. К данным сетям относятся сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен информацией (передачу сообщений) между компьютерными устройствами. При этом не имеет значения количество компьютерных устройств, входящих в технологичную систему, и пользователей, имеющих к ней подключение. Использование указанных устройств и сетей позволяет реализовать более сложные схемы преступной деятельности, которые сложно повторить при личном общении, а дистанционный (удаленный) формат общения, являясь самым простым способом анонимизации личности, минимизирует риск быть идентифицированным.

В последнее время становится популярным мошенничество с применением навыков «социальной инженерии»[1]. Ставшие уже известными широкой общественности звонки от «сотрудников службы безопасности банка» и «попавших в беду родственников» не прекращаются и по сей день. До недавнего времени такие звонки совершались в значительной части лицами, отбывающими наказание в местах лишения свободы[2]. Так, осужденный, отбывающий наказание в ФКУ <…> ГУФСИН России, используя мобильный телефон, совершил 188 фактов мошенничества. Также есть данные о лицах, совершивших 173, 95 и 52 мошенничества[3]. К сожалению, большинство таких преступлений остаются нераскрытыми. В настоящее время более 90 % звонков поступают из колл-центра, расположенного на территории Украины, как правило, это город Днепр.

---

[1] Панфилова О. А. Некоторые вопросы обеспечения безопасности на объектах уголовно-исполнительной системы и организации борьбы с телефонными мошенничествами // Вестник Воронежского института ФСИН России. 2022. № 3. С. 107–115.

[2] Алескеров В. И., Колокольчикова О. Н., Василенко Л. В., Ломакин С. Н. Сфера телекоммуникаций и компьютерной информации как платформа для совершения современных видов преступлений : учеб.-практ. пособие. Домодедово : ВИПК МВД России, 2021. С. 122–125.

[3] Литвинов Н. Д., Федоров А. Н. Особенности, причины и тенденции развития дистанционного мошенничества лицами, отбывающими наказание в местах лишения свободы // Научно-исследовательские публикации. 2015. № 12 (32). С. 63–72.

Есть даже информация, что задействована служба безопасности Украины, контролирующая все моменты, связанные с хищениями[1].

Мобильные телефоны, компьютерные устройства, подключенные к информационно-телекоммуникационным сетям, дают возможность использовать разнообразные современные способы совершения преступлений. Назовем некоторые из них.

1. Изменение номера вызывающего абонента. В этом случае преступники присваивают официальные номера, используемые банками или другими государственными учреждениями, например номер «900».

Для изменения идентификационного номера вызывающего абонента используют возможности технологий VoIP (Voice over Internet Protocol) или IP-телефонии, позволяющие пользователям совершать звонки через сеть Интернет и изменять идентификатор вызывающего абонента на любой номер по своему выбору, а также аппаратных спуфинговых (spoofing) устройств.

Более того, в сети Интернет существуют организации, оказывающие услуги подделки идентификатора вызывающего абонента, позволяя пользователям вводить номер, который они хотят отобразить, и номер, на который они хотят позвонить.

Некоторые телефонные компании, предлагающие услуги аутентификации по идентификатору вызывающего абонента, проверяют идентификатор вызывающего абонента для входящих вызовов и предупреждают получателя, если идентификатор вызывающего абонента является поддельным.

2. Осуществление генерации голоса человека с помощью технологии искусственного интеллекта. Для этого используется программное обеспечение, которое создает реалистичные искусственные голоса на основе анализа и синтеза звуков.

3. Использование технологии голосовых вызовов через сеть Интернет посредством популярных мессенджеров, таких как:

– Viber – с 2014 года принадлежит японской e-commerce-компании «Rakuten» со штаб-квартирой в Токио;

– WhatsApp – американский бесплатный сервис обмена мгновенными сообщениями и голосовой связи по IP, принадлежащий компании Meta[2] (США);

– VK-мессенджер – ООО «ВК» (Россия);

– Telegram – кроссплатформенная система мгновенного обмена сообщениями (мессенджер) с функциями обмена текстовыми, голосовы-

---

[1] Более 90 процентов мошеннических звонков красноярцам поступает с территории Украины // Новости Красноярского края – события, анонсы, происшествия, афиша, погода : сайт. URL: https://gnkk.ru/news/bolee-90-procentov-moshennicheskikh-zvonk/.

[2] Использование на территории Российской Федерации ограничено.

ми и видеосообщениями, стикерами и фотографиями, файлами многих форматов (офисы Telegram расположены в Дубае, компания находится в юрисдикциях Германии, Великобритании);

– Facebook[1] Messenger – приложение для обмена мгновенными сообщениями и видео, созданное Meta;

– Wire – это зашифрованное приложение для общения и совместной работы, созданное Wire Swiss (Германия);

– Signal – официальный собственник мессенджера фонд Signal Technology Foundation (США);

– WeChat – мобильная коммуникационная система для передачи текстовых и голосовых сообщений, разработанная компанией Tencent (Китай);

– Discord – кроссплатформенная проприетарная система мгновенного обмена сообщениями (мессенджер) с поддержкой VoIP и видеоконференций, предназначенная для использования различными сообществами по интересам. Разработчиком является компания Discord Inc. (США).

В данный перечень включены наиболее популярные сегодня на территории России мессенджеры. Для преступников есть ряд преимуществ в использовании данных систем для телефонных звонков и текстовых сообщений. При осуществлении звонка или отправке текстовых сообщений непосредственно через оператора связи последний, в соответствии с законодательством (ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[2] (далее – ФЗ «О связи»)), обязан в течение 3-х лет хранить информацию о действиях абонента (звонки, смс и их дата, адресат и т. п.), а также до полугода хранить запись разговора, содержание сообщений или пересылаемые медиафайлы, т. е. исчерпывающую информацию обо всех действиях, которые осуществлял абонент. Данные сведения предоставляются правоохранительным органам и могут использоваться в качестве доказательств преступной деятельности либо служить вспомогательной оперативной информацией. Указанные требования обязательны для исполнения зарегистрированными операторами связи, осуществляющими деятельность на территории Российской Федерации.

В случае использования мессенджеров при совершении преступлений или при общении преступников между собой от оператора связи реально получить только информацию об использовании интернет-трафика и о том, на какие серверы поступает и откуда приходит информация. Получение содержания разговора и текстового сообщения затруднительно. Во-первых, почти все популярные мессенджеры расположены за преде-

---

[1] Использование на территории Российской Федерации ограничено.

[2] О связи : Федер. закон № 126-ФЗ : принят Гос. Думой 18 июня 2003 г. : одобрен Советом Федерации 25 июня 2003 г. : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_43224/.

лами Российской Федерации, поэтому реализовать это сложно, несмотря на законодательно закрепленную обязанность хранить и предоставлять правоохранительным органам информацию, передаваемую в мессенджерах, а в условиях санкционной политики некоторых государств по отношению к России и вовсе невозможно. Во-вторых, существует реальная возможность использования уникальных, созданных специально для отдельной группы людей мессенджеров, в которых преступники могут обмениваться информацией о своей преступной деятельности[1]. При передаче сообщений в таких мессенджерах используется шифрование end-to-end (E2E – оконченное или сквозное). Перехватить и расшифровать такие сообщения (информацию) без соответствующих ключей технически достаточно трудно. То есть преступники либо покупают такие приложения и настраивают для собственного использования, либо, обладая профессиональными знаниями, используя открытый код программистов, компилируют и оптимизируют такое приложение самостоятельно. Сайт github.com – самый массовый на сегодняшний день ресурс, содержащий огромный массив информации, в том числе интересные решения для шифрования, которые используются преступниками. Запрос на предоставление необходимой информации и (или) ключей для расшифровки правоохранительным органам фактически некому отправить, поскольку «собственное» приложение нигде не регистрируется и используется ограниченным числом участников.

4. Настройка функционала мессенджера, создающая видимость принадлежности к какой-либо организации, например банку, с использованием официального логотипа этой организации.

5. Использование мессенджера, например Telegram, позволяет автоматизировать рутинные процессы. В Telegram достаточно популярны специальные аккаунты, которые позволяют осуществлять автоматическую обработку данных. Такие аккаунты именуют «Bot» (виртуальный робот, робот-бот). Данный «Bot» не имеет привязки к конкретному пользователю, но в то же время предоставляет возможность общения с пользователями. Телеграм-бот не требует постоянного нахождения человека за компьютером, автономно, по заданному алгоритму выполняет различные действия, что значительно снижает количество точек соприкосновения между участниками сообществ, а также затрудняет выявление их деятельности[2].

---

[1] Девяткин Г. С., Луценко П. А. Переписка в мессенджерах и социальных сетях как доказательство по уголовному делу // Государственная служба и кадры. 2021. № 2. С. 159–161.

[2] Гаврилин Ю. В. Противодействие цифровой трансформации наркопреступности (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 4 (56). С. 122–129.

6. Изменение IP-адреса, который представляет собой уникальный идентификатор, назначенный каждому устройству, подключенному к сети Интернет. Этот адрес используется для маршрутизации данных между устройствами в сети. IP-адрес может дать представление о местоположении устройства, связанного с сетью Интернет, однако многие интернет-провайдеры используют метод маскирования IP-адресов, так что местоположение устройства, определенное по IP-адресу, может быть неточным. Кроме того, IP-адрес не привязан к конкретному человеку, использующему это устройство, а также одно и то же устройство (общий компьютер в интернет-кафе и т. д.) могут использовать несколько человек.

Для возможности идентификации человека по IP-адресу необходима дополнительная информация, такая как имя пользователя и пароль для входа в систему, либо информация из браузера или других используемых преступником приложений.

7. Использование технологии геолокации, позволяющей определить местоположение устройств в Интернете, их IP-адреса, подключенные сети Wi-Fi.

8. Использование метаданных. Граждане, пользующиеся современными ИТ-технологиями для своих целей, либо представители компаний размещают огромный массив данных о себе или о своей организации. Это могут быть текстовые файлы, схемы, чертежи, фотографии, видео, какие-либо программы. Анализ метаданных позволяет получить ценную информацию о потенциальных потерпевших. Если это физическое лицо, в зависимости от типа файла можно узнать различную информацию. Для фотографий это модель устройства, с помощью которого сделано фото, и его технические характеристики; размер фотографии; дата и время съемки; геолокация, если у камеры есть доступ к ней; автор фотографии; расстояние от камеры в момент съемки; теги и ключевые слова, описывающие содержание фото (создаются автором). Для видеофайлов набор идентичный и может дополняться в зависимости от модели устройства. Текстовые файлы содержат следующую информацию: автор документа (если пользователь его указал); формат файла; название файла; даты создания и редактирования файла; размер файла. Важен и сам способ передачи файлов. Если файлы передаются через почтовые сервисы (Gmail, Яндекс.Почта, Mail.ru, Protonmail), то они остаются неизменными, соответственно, метаданные сохраняются в полном объеме. Если используются мессенджеры, как правило, есть два варианта передачи: «отправить как фото» и «отправить как файл». При отправке фотографии как «файла» метаданные остаются, а при отправке «как фото» – большинство популярных мессенджеров удаляют метаданные с отправляемых изображений.

Если же деятельность преступников направлена на сайт или приложение какой-либо организации, метаданные с этих источников могут

содержать информацию об адресе корпоративной электронной почты, операционной системе, которую используют сотрудники организации, и т. п. Эта информация может помочь преступникам осуществить различные виды атак с использованием методов социальной инженерии (например, зная модель фотоаппарата, можно завести разговор с фотолюбителем, или же сделать рассылку писем с вредоносным ПО на адреса электронной почты работников определенной организации).

9. Использование личной информации из социальных сетей. Многие пользователи добровольно размещают в социальных сетях личную информацию: Ф.И.О.; возраст; образование; школа и институт, в которых обучался человек; год обучения и факультет (класс); религиозные убеждения; увлечения; статусы (краткие заметки) и т. д. С возрастом или трудоустройством в какую-либо организацию или с занятием ответственной должности пользователи часто корректируют либо вообще удаляют информацию о себе. Однако не все пользователи осведомлены о существовании так называемого «Архива Интернета» (англ. Internet Archive) – некоммерческой организации, основанной в 1990-х годах в США. Главной заявленной целью Архива является предоставление всеобщего доступа к накопленной в Интернете информации. Коллекция Архива Интернета состоит из множества подколлекций архивированных веб-сайтов, оцифрованных книг, аудио- и видеофайлов, игр, программного обеспечения. Один из проектов Архива Интернета – это сервис Wayback Machine, расположенный по адресу http://web.archive.org/. Данный сервис периодически сохраняет страницы в сети Интернет. При изменении информации или даже удалении самой страницы она остается в архивах сервиса. Введя адрес сайта, можно посмотреть, на какие даты есть «снимки» сайта, и просмотреть их. Полученная таким образом информация также может быть использована для атак с использованием методов социальной инженерии, в том числе для шантажа лица распространением нежелательной информации о нем.

10. Перехват сообщений в мессенджерах, перехват трафика в сети. Один из способов – взлом аккаунта пользователя. Преступники могут пытаться получить доступ к аккаунту, используя уязвимости в программном обеспечении или социальные инженерные атаки, такие как подделка веб-сайтов или фишинговые электронные письма. В этом случае преступник создает фальшивую страницу входа на сайт или приложение, которая по визуальному оформлению похожа на официальную платформу, и просит пользователя ввести учетные данные для входа. Как только пользователь вводит свои учетные данные, преступник получает доступ к его учетной записи и может перехватить информацию, находящуюся на платформе (персональные данные, сообщения, номера банковских карт), а также воспользоваться личным кабинетом гражданина и осуществлять преступные действия от его имени.

Для защиты от фишинга важно всегда проверять адрес веб-сайта, прежде чем вводить учетные данные, и быть осторожным с электронными письмами или сообщениями, в которых запрашивается конфиденциальная информация. Кроме того, использование двухфакторной аутентификации и регулярная смена паролей также могут повысить безопасность пользователя.

Для перехвата трафика в сети могут также использоваться шпионские программы или промежуточные прокси-серверы, чтобы перехватывать и читать переписку. Например, атаки «человек посередине» (от англ. Man-in-the-middle, MITM) – распространенный метод, используемый преступниками для перехвата сообщений в платформах обмена мгновенными сообщениями. Этот тип атаки заключается в том, что злоумышленник перехватывает связь между двумя пользователями, обычно путем создания поддельной сети, которая кажется истинной сетью, и обманом заставляет пользователя подключиться к ней. Как только пользователь подключается к поддельной сети, преступник получает доступ к конфиденциальной информации, включая сообщения, отправленные через платформу обмена мгновенными сообщениями.

Для защиты от MITM-атак важно использовать безопасные сети, такие как виртуальные частные сети (VPN), которые шифруют данные, передаваемые через сеть Интернет. Кроме того, использование шифрования на платформах обмена мгновенными сообщениями также может помочь защититься от этих атак. Обнаружить данный тип атаки можно по следующим признакам: неожиданное или повторяющееся отклонение от доступа к странице, поскольку преступники принудительно отключают пользователей, чтобы перехватить имя пользователя и пароль при повторной попытке подключения; подозрительные адреса в строке браузера, например, www.go0gle.com вместо www.google.com, что свидетельствует о перехвате DNS[1].

11. Вредоносное ПО – это тип программного обеспечения, предназначенный для причинения вреда компьютеру или устройству. Использование вредоносного ПО в преступных целях позволяет получить доступ к устройству пользователя и конфиденциальной информации, включая сообщения, отправляемые через платформы обмена мгновенными сообщениями.

12. Использование программ для удаленного доступа к телефону. Данные программы позволяют получить физический контроль над устройством (при оказании помощи в настройке телефона, установке приложений и т. п.), а также возможность удаления учетной записи при обнаружении устройства правоохранительными органами. Данный способ

[1] Man-in-the-Middle: советы по обнаружению и предотвращению // Хабр : веб-сайт. URL: https://habr.com/ru/companies/varonis/articles/526632/.

используется при совершении телефонного мошенничества. Например, пользователю поступает телефонный звонок, в котором мошенник сообщает о том, что неизвестное лицо из другого региона пытается войти в его личный кабинет приложения банка ВТБ. Преступники, выясняя информацию об использовании приложения банка, сведения о его обновлении, отправляют СМС-сообщение с кодом и требуют подтверждения факта получения такого СМС и дальнейшего обновления используемого приложения.

При использовании в устройстве операционной системы Android клиенту предлагают войти в магазин приложений Google Play, найти и скачать приложение «Поддержка ВТБ». На данный запрос пользователю в первую очередь предлагается скачать приложения (например, RustDesk Remote Desktop (рис. 1)) для удаленного управления устройством, установление которого и его активация абонентом путем ввода кода дает преступнику возможность получить удаленный контроль над смартфоном и произвести любые доступные операции (хищение персональных данных, перевод денег с приложений банков, рассылка писем от имени банка и т. п.).

13. Использование незащищенных сетей Wi-Fi, позволяющих осуществить перехват сообщений. Если пользователь получает доступ к платформе обмена мгновенными сообщениями через незащищенную сеть Wi-Fi, его сообщения могут быть перехвачены злоумышленником в той же сети.

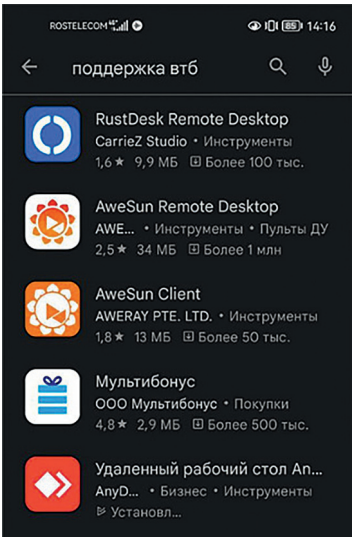


Рис. 1. Ответ на запрос «Поддержка ВТБ» в магазине приложений Google Play

Преступники могут взломать сеть Wi-Fi. Взлом Wi-Fi – это процесс доступа к ресурсам сети или кражи конфиденциальной информации. Существует несколько стандартов сетей Wi-Fi – WEP, WPA / WPA2, WPA3, сменяющих друг друга для обеспечения безопасности пользователей и увеличения скорости, но не все компьютерные устройства поддерживают современные стандарты, обеспечивающие безопасное пользование. Кроме того, WEP – это устаревший протокол безопасности, который легко взламывается, а WPA и WPA2 – защищенный доступ Wi-Fi, являясь более безопасными протоколами, все же могут быть уязвимы для атак, если сетевой пароль слаб или сеть настроена неправильно. WPA3 – это новый стандарт безопасности Wi-Fi-сетей, представленный Wi-Fi Alliance в 2018 году, который является наиболее защищенным.

Возможно создать и фальшивую сеть Wi-Fi с именем, похожим на настоящую сеть Wi-Fi (атака «злой двойник» (Evil Twin Attack)), при подключении к которой предоставляется доступ к информации, хранящейся на компьютерном устройстве.

14. Использование средств анонимизации в сегменте DarkNet. Один из самых популярных на сегодняшний день интернет-браузеров – «TOR» (The Onion Router) – бесплатный веб-браузер с открытым исходным кодом, который предназначен для защиты конфиденциальности и анонимности пользователей при просмотре веб-страниц. Он работает путем маршрутизации интернет-трафика через сеть серверов, также известных как узлы, таким образом, что кому-либо (в том числе правоохранительным органам) становится трудно отслеживать онлайн-активность пользователя или его физическое местоположение. TOR базируется на принципе луковой маршрутизации, который позволяет передавать данные через сеть узлов (нод), чтобы путь нельзя было отследить. Каждый узел в сети TOR представляет собой промежуточный пункт для передачи данных, которые затем передаются далее до конечной цели. Это означает, что никто не может узнать источник или пункт назначения данных, так как каждый узел в сети видит только предыдущий и следующий узлы, а не источник и пункт назначения. Браузер TOR шифрует интернет-трафик пользователя и обертывает его несколькими слоями шифрования, аналогично onion, что затрудняет перехват и чтение интернет-трафика пользователя. Зашифрованный трафик затем маршрутизируется через ряд узлов в сети TOR. Каждый узел в сети удаляет один уровень шифрования, а затем передает трафик следующему узлу. Конечный узел в сети, известный как узел выхода, расшифровывает трафик и отправляет его на целевой веб-сайт. Узел выхода действует как прокси-сервер пользователя, поэтому при анализе информации о взаимодействии с ресурсом отображается трафик, поступающий с узла выхода, а не с устройства пользователя. Поскольку интернет-трафик пользователя маршрутизируется через несколько узлов сети, веб-сайт может видеть только

IP-адрес выходного узла, а не фактический IP-адрес пользователя. Это затрудняет отслеживание физического местоположения пользователя.

С точки зрения конфиденциальности и анонимности браузер TOR обеспечивает высокую степень защиты, но он не является надежным. Например, если пользователь посещает веб-сайт, который требует от него ввода личной информации, такой как его имя и адрес, эта информация все равно может быть отслежена и связана с пользователем. Более того, хотя сеть TOR и обеспечивает защиту от сетевого наблюдения и анализа трафика, она не обеспечивает защиту от сквозных временных атак, которые могут быть использованы для получения информации о поведении пользователя в сети Интернет.

Для успешного выявления, расследования и предупреждения преступлений, совершаемых с использованием ИТТ, правоохранительные органы используют различные методы и программные, технические и тактические средства, которые будут рассмотрены во второй главе настоящего пособия. А сейчас акцентируем внимание на основных признаках, по которым можно предположить о совершенном или совершаемом с использованием ИТ-технологий преступлении:

1. Измененный адрес URL на сайте: преступники могут создавать зеркальные сайты (клоны подлинных), используя незначительные изменения в адресе URL.

2. Обнаружение необычной (несвойственной) активности на личных аккаунтах. Преступники могут получить доступ к аккаунтам пользователей в том случае, если последние использовали один и тот же логин (как правило, адрес почты либо номер телефона) и пароль. Обнаружить подобные действия возможно через просмотр и анализ истории активных сеансов аккаунта, а также через уведомления на телефон.

3. Подозрительные действия в онлайн-банкинге. Зафиксированные пользователем движения по банковскому счету, которых он не совершал. Например, появление нулевого баланса или отображение операций – подобное может указывать на деятельность мошенников.

4. Сообщения в мессенджерах либо электронной почте, которые на устройстве отмечены как прочитанные (в случаях, если в действительности пользователем они не просматривались). Подобное может также свидетельствовать о деятельности преступников.

5. Поддельные смс-сообщения, которые отправляются преступниками, но отображаются как сообщения от банков или других сервисов. В них может быть сказано о необходимости внесения дополнительной информации для восстановления аккаунта.

Современные информационно-телекоммуникационные технологии внесли свои коррективы в развитие преступного мира. На сегодняшний день способов совершения преступлений с использованием указанных технологий большое количество. Перечень этих способов не являет-

ся исчерпывающим, цель данного пособия – показать их разнообразие по механизму следообразования и принципу действия: от простого телефонного мошенничества до сложных манипуляций по проведению фишинговых атак и перехвату трафика в сети Интернет. Безусловно, знание сотрудниками органов внутренних дел основных способов совершения противоправных деяний важно для эффективного осуществления деятельности, направленной на раскрытие, расследование и предупреждение преступлений.

Такие знания позволяют следователям незамедлительно принимать тактические решения о проведении следственных, процессуальных действий или применении мер процессуального принуждения. Например, в некоторых следственных подразделениях г. Москвы сложилась положительная практика ареста банковских счетов, используемых при совершении указанных преступлений, в течение трех суток с момента возбуждения уголовного дела (в порядке ч. 5 ст. 165 УПК РФ). Арест счетов злоумышленников позволяет обеспечить возможность возмещения ущерба потерпевшим. В данном случае удается не только лишить преступников возможности распоряжаться похищенными деньгами, но и незамедлительно пресекать совершение преступлений[1]. Однако следует учитывать, что подобные действия сотрудников правоохранительных органов могут применяться эффективно только при условии компетентности следователей в рассматриваемой области, и далеко не каждый следователь возьмет на себя такую ответственность, как арест банковских счетов в порядке ч. 5 ст. 165 УПК РФ.

Резюмируя изложенное, считаем целесообразным отметить, что, несмотря на наличие в системе правоохранительных органов специалистов и процессуально закрепленной возможности использования консультативной помощи лиц, обладающих специальными знаниями, этих механизмов в реальности зачастую недостаточно. Для обеспечения эффективной деятельности органов следствия и дознания при их работе с электронными устройствами и компьютерной информацией необходимо, но не всегда возможно осуществлять постоянное взаимодействие с различного рода специалистами в области ИТ-технологий. В настоящее время, на наш взгляд, наиболее рациональным и действенным решением сложившейся ситуации является повышение уровня профессиональных знаний тех лиц, которые непосредственно занимаются раскрытием и расследованием рассматриваемых преступлений. Наличие у таких сотрудников знаний в области ИТ-технологий многократно повысит уровень расследования, что в дальнейшем может способствовать своевременному предупреждению подобных противоправных деяний.

---

[1] Информационное письмо прокуратуры г. Москвы № 16/6-17-2022/16861-22-20450016.

Контрольные вопросы

1. Как в криминалистике понимается механизм преступления и его соотношение со способом преступления?
2. Перечислите основные способы совершения преступлений с использованием ИТТ и охарактеризуйте возможности используемых технологий.
3. Перечислите наиболее распространенные среди пользователей в Российской Федерации мессенджеры и назовите преимущества их использования в общении.
4. Значение IP-адреса в установлении механизма преступления.
5. Какую информацию получают преступники, изучая социальные сети?
6. Какие существуют стандарты сетей Wi-Fi? Перечислите их отличия.
7. Особенности использования интернет-браузера «TOR» при совершении преступлений с использованием ИТТ.
8. Какая криминалистически значимая информация может быть получена при изучении метаданных различных типов файлов?

ГЛАВА 2. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ АСПЕКТЫ ПРОВЕДЕНИЯ ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Общие принципы производства следственных действий при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Комплекс следственных и иных действий, проводимых при расследовании преступлений, совершенных с использованием ИТ-технологий, в значительной мере зависит от конкретного вида преступного деяния, его уголовно-правовой квалификации и сложившейся следственной ситуации.

Под следственной ситуацией в криминалистике принято понимать совокупность условий информационного, уголовно-процессуального и тактического характера, сформировавшихся на определенном этапе расследования. Ситуационный подход как криминалистическое учение позволяет субъектам правоприменения определять типичные тактические и иные приемы, способные разрешать конкретную ситуацию расследования и правильно управлять ею. Следственные ситуации первоначального этапа расследования рассматриваемых ранее классификационных групп преступлений зависят от информационной осведомленности следователя о преступлении, что относится к объективным факторам.

Информационная осведомленность зависит от наличия криминалистически значимой и доказательственной информации или возможности ее получения. Возможность получения такой информации определяется не только познавательной активностью следователя при проведении следственного действия, но и характеристикой цифровых следов. Риск уничтожения криминалистически значимой информации связан с техническими условиями и нормативными сроками ее хранения.

Технические условия хранения зависят от характеристик компьютерного устройства (объема его памяти, настроек операционной системы

и т. п.). Нормативные сроки хранения зависят от действующего законодательства, определяющего сроки хранения определенного вида информации.

При расследовании преступлений, совершенных с использованием ИТТ, формируются следующие типичные следственные ситуации:

1) известны только преступные последствия преступлений, и не известно лицо, совершившее преступление;

2) известна часть обстоятельств совершения преступления, но не известно виновное лицо;

3) известны обстоятельства совершения преступления и виновное лицо[1].

Кроме того, выделяют и другие классификации следственных ситуаций, которые могут быть представлены следующим образом:

1. В зависимости от осведомленности владельца:

– владелец компьютерной информации и имущества самостоятельно выявил факт неправомерного доступа к ней или факт ее ввода, удаления, блокирования, модификации или иного вмешательства в функционирование средств ее хранения, обработки или передачи, повлекшего хищение его имущества, а также кражу с банковского счета или в отношении электронных денежных средств;

– факт совершения преступлений рассматриваемой группы выявлен правоохранительными органами.

2. В зависимости от наличия сведений об использовании различных компьютерных устройств при совершении преступлений:

– ситуации, когда при совершении преступлений использовались компьютерные устройства;

– ситуации, когда при совершении преступлений использовались электронные или информационно-телекоммуникационные сети (включая сеть Интернет);

– ситуации, когда в ходе совершения преступлений компьютерные устройства использовались как средство взаимодействия между соучастниками, а также для хранения, обработки, передачи информации;

– ситуации, когда компьютерные устройства являются предметом преступления.

При этом следует помнить, что сочетание комбинаций этих ситуаций может быть различным, они могут переходить из одной в другую, конкретизироваться или детализироваться. С учетом сложившихся следственных ситуаций следователь определяет последовательность следственных

---

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений : дис. … канд. юрид. наук. Москва, 2016. С. 67.

действий и принимает решение о тактических приемах их проведения. Следует отметить, что чаще всего следственные ситуации при расследовании рассматриваемых преступлений характеризуются дефицитом ориентирующей, криминалистически значимой и доказательственной информации, обусловленным специфичностью способа преступления и механизма следообразования, сложностью обнаружения и сохранения цифровых следов. Поэтому следователь должен обладать соответствующими знаниями о тактических приемах проведения следственных действий, направленных на отыскание и изъятие таких следов.

В этой связи последовательность следственных действий определяется с учетом их поисковых возможностей обнаружения, фиксации и изъятия криминалистически значимой информации и доказательств.

В этой связи в первую очередь необходимо проводить следственные действия, направленные на:

– получение информации от непосредственных участников преступления и иных лиц, которым известны какие-либо сведения, имеющие криминалистическое значение;

– получение информации об информационно-телекоммуникационных средствах, которые использовались в ходе совершения преступления, и изъятие электронных носителей информации и компьютерной информации;

– получение иных сведений, входящих в предмет доказывания по уголовному делу.

Основные тактические цели этих следственных действий будут сводиться к установлению электронного носителя информации, обнаружению на нем следов материальных и цифровых, их изъятию и дальнейшему исследованию.

Кроме того, на формирование следственной ситуации влияют и субъективные факторы, к которым следует отнести:

– наличие у следователя соответствующей квалификации и опыта по расследованию преступлений, совершенных с использованием информационных технологий;

– наличие фактов и возможностей противодействия расследованию со стороны подозреваемых и других заинтересованных лиц;

– наличие ошибок в планировании и проведении следственных действий, оперативно-розыскных мероприятий, действий участников расследования.

Следователь, специализирующийся на расследовании преступлений, совершенных с использованием информационных технологий, должен обладать знаниями в области функционирования информационных систем, компьютерных устройств, понимать их возможности для хранения, обработки и передачи информации. Если следователь ими не обладает, то подготовка и проведение следственных действий будут характеризоваться

ситуацией неопределенности[1], провоцирующей возникновение ошибок планирования, определения очередности и выбора тактики их проведения. И наоборот, наличие таких знаний у следователя будет способствовать преодолению активного противодействия со стороны подозреваемого в ходе проведения следственных действий.

В теории криминалистики под противодействием расследованию понимают деятельность причастных к преступлению и иных заинтересованных лиц, осуществляемую с целью уклонения от ответственности или смягчения наказания; деятельность по воспрепятствованию решению задач уголовного судопроизводства посредством воздействия на процесс расследования, криминалистически значимую информацию и ее носители[2].

Следует отметить, что противодействие расследованию преступлений, совершенных с использованием ИТТ, осуществляется прежде всего с использованием при совершении преступления средств анонимизации лицами, их совершившими, в том числе путем удаленного или дистанционного воздействия на компьютерное устройство с целью уничтожения цифровых следов преступления.

В этой связи тактически правильные действия следователя могут способствовать выявлению и преодолению противодействия расследованию.

Тактико-криминалистические рекомендации по проведению отдельных следственных действий обладают общими чертами, характерными для рассматриваемой категории преступлений.

В первую очередь перед следователем стоит задача принятия тактического решения по определению программы и последовательности действий. Ключевым звеном в определении этой последовательности является программно-целевой процесс планирования расследования. Планирование расследования преступлений, совершенных с использованием ИТТ, осуществляется в условиях информационного дефицита. Поэтому следователь, разрабатывая план расследования, должен определить возможные источники получения криминалистически значимой и доказательственной информации, учесть их характеристики, влияющие на сохранность и идентификационный период цифровых следов, а также возможные риски уничтожения информации.

При планировании проведения следственных действий, направленных на получение информации от непосредственных участников пре-

---

[1] Рудых А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : дис. … канд. юрид. наук. Ростов н/Д, 2019. С. 96.

[2] Грибунов О. П., Унжакова С. В. Противодействие расследованию преступлений и меры по его преодолению : учеб. пособие. Иркутск : ФГКОУ ВО ВСИ МВД России, 2019. С. 14.

ступления и иных лиц, которым известны какие-либо сведения, имеющие криминалистическое значение, следователю необходимо изучить имеющуюся информацию о преступном событии, определить предмет допроса участников уголовного судопроизводства, спрогнозировать возможное их поведение, с учетом которого определить необходимость применения тактических приемов, а также привлечь необходимого специалиста.

При планировании следственных действий, направленных на получение информации об информационно-телекоммуникационных средствах, использованных в ходе совершения преступления, и изъятие электронных носителей информации и компьютерной информации, следует акцентировать внимание на определении необходимости привлечения специалиста с учетом профильности его специальных знаний, подготовки криминалистических, программно-аппаратных средств, средств хранения информации (жесткий диск или несколько дисков суммарной емкостью не меньше, чем копируемый НЖМД), средств устранения угрозы информационной безопасности, средств подавления радиосигналов, средств, поглощающих электромагнитные излучения, или средств экранирования помещений и т. п.

Планирование проведения следственных действий, направленных на получение иных сведений, входящих в предмет доказывания по уголовному делу сводится к изучению исходной информации о преступлении, определению задач, которые следует решить в рамках следственного действия, круга необходимых участников, места и времени проведения следственного действия, тактических приемов, обеспечивающих решение поставленных задач, с учетом возможного поведения лиц, участвующих в следственном действии.

Готовность следователя к проведению следственного действия во многом определяет его эффективность.

Кроме того, результативность следственного действия и его доказательственное значение зависят от соблюдения общих тактических рекомендаций, к которым относятся:

– соблюдение принципа законности;

– своевременность принятия тактического решения о проведении следственного действия;

– учет особенностей преступления, по которому проводится следственное действие;

– обеспечение единства руководства процессом проведения следственного действия;

– проявление активности и целеустремленности лица, его производящего;

– комплексное эффективное использование технико-криминалистических средств и сил взаимодействующих субъектов.

В целях соблюдения общих тактических рекомендаций, в первую очередь законности и комплексного использования сил, при проведении следственных действий в ходе расследования преступлений, совершенных с использованием ИТТ, следователю следует обратить особое внимание на положения ч. 2 ст. 164.1 УПК РФ. Изъятие СКТ, ЭНИ и компьютерной информации должно происходить при непосредственном участии соответствующих специалистов.

Специалист – это лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию. Использование ИТТ в преступной деятельности определяет необходимость привлечения специалиста при проведении следственных действий, прежде всего направленных на обнаружение, фиксацию и изъятие цифровых следов, ЭНИ, а также при проведении допроса участников уголовного судопроизводства. Кроме того, нередко возникает необходимость допроса и самого специалиста.

Привлеченный к следственному действию специалист должен быть компетентным, то есть обладать соответствующими специальными знаниями, чем следователь, в соответствии с ч. 2 ст. 168 УПК РФ, должен удостовериться до начала следственного действия. В соответствии с приказом МВД России от 11 января 2009 г. № 7 «Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России»[1], по получении указания дознавателя, следователя или суда о направлении специалиста для участия в процессуальном действии руководитель экспертно-криминалистического подразделения обязан поручить участие в его проведении конкретному сотруднику, обладающему специальными познаниями в объеме, требуемом для оказания необходимого содействия.

При расследовании рассматриваемых преступлений к специальным знаниям специалиста могут относиться знания:

– по компьютерной безопасности;
– по операционным системам;
– по сетевым технологиям;
– по средствам связи и коммуникации;
– по системному администрированию;

[1] Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России : приказ МВД России от 11 января 2009 г. № 7 : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=451495#pzXLE4Ua0ErMq1d5.

– по разработке программного обеспечения;
– по экономике, бухгалтерскому учету;
– по криминалистике[1].

Принято понимать, что компетентность формируют образование, умения, навыки и опыт работы. Такой поход к пониманию компетентности используется и в правоприменительной практике, т. е. компетентность специалиста определяется наличием у него соответствующего образования, стажа и опыта работы по соответствующей специальности.

Специалист может быть привлечен как из системы МВД России, так и из сторонней организации, в этом случае в материалах дела его компетентность должна найти отражение в виде копий соответствующих документов, например диплома об образовании или трудовой книжки. Конечно, желательно, чтобы в качестве специалиста привлекался эксперт ЭКЦ МВД России субъекта Российской Федерации, имеющий право на производство компьютерной и радиотехнической экспертиз. Однако обеспечить существующую потребность участия профильного специалиста в следственных, процессуальных действиях фактически невозможно. В этой связи, в соответствии с п. 16.8 приказа МВД России от 9 января 2013 г. № 2[2], при получении экспертом права на участие в качестве специалиста в процессуальных действиях и оперативно-розыскных мероприятиях им приобретаются навыки работы с электронными носителями информации, компьютерной и иной техникой. Поэтому следователь, исходя из способа совершения преступления, фактически оценивая технологическую сложность изымаемого и осматриваемого технического устройства, определяет необходимый уровень профессиональной компетентности специалиста для его участия в следственном действии. А руководитель экспертно-криминалистического подразделения при получении соответствующего указания от следователя должен поручить участие в его проведении конкретному специалисту, обладающему специальными знаниями в требуемом для оказания содействия объеме (приказ МВД России от 11 января 2009 г. № 7).

---

[1] Колычева А. Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. … канд. юрид. наук. Москва, 2018. С. 110.

[2] Вопросы определения уровня профессиональной подготовки экспертов в системе МВД России» (вместе с «Положением об аттестации экспертов на право самостоятельного производства судебных экспертиз и о порядке пересмотра уровня их профессиональной подготовки в системе Министерства внутренних дел Российской Федерации», «Положением о Центральной экспертно-квалификационной комиссии Министерства внутренних дел Российской Федерации») : приказ МВД России от 9 января 2013 г. № 2 : ред. от 27.09.2023 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_145829/.

В теории же вопросы привлечения специалиста становятся предметом дискуссий с точки зрения необходимости его участия в следственных действиях. Закрепленная в УПК РФ обязанность привлекать специалиста, с одной стороны, является обоснованной в части необходимости оказания помощи следователю при работе с электронными носителями информации для сохранения цифровой криминалистически значимой информации и следов преступления на носителе, а с другой – является чрезмерной, когда осуществляется изъятие самого простого по своему функциональному предназначению носителя информации (например, флеш-карты).

В исследованиях можно наблюдать разнообразные мнения по соблюдению этого процессуального требования. Вопрос о необходимости привлечения специалиста решается в зависимости:

– от типа изымаемого носителя;

– от наличия реальной необходимости использования его знаний при изъятии;

– от сферы совершаемых преступлений[1].

С последним, столь избирательным, подходом трудно согласиться. Привлечение специалиста в зависимости от реальной необходимости или типа изымаемого электронного носителя выглядит вполне логичным. При этом аргументация неисполнения требований УПК РФ в рассматриваемом вопросе сводится к тому, что для изъятия ЭНИ, таких как флеш-карты, жесткие диски, телефоны, ноутбуки и другие подобные объекты, не требуется специальных знаний, а необходимость их использования возникает при копировании информации. Такую же позицию можем наблюдать и в решениях судов.

Так, Верховный Суд Российской Федерации определением от 14 ноября 2019 г. оставил без удовлетворения апелляционную жалобу, поступившую от стороны защиты, об оспаривании приговора суда о виновности гр. А. в осуществлении деятельности организации («Исламское государство»), которая в соответствии с законодательством Российской Федерации признана террористической; в незаконном приобретении, хранении и ношении огнестрельного оружия и боеприпасов; в приготовлении к убийству двух и более лиц по мотиву религиозной ненависти, ходатайствовал в том числе о признании недопустимым доказательством результатов обыска (выемки) мобильного телефона, который производился без участия специалиста, что является нарушением требований закона. В апелляционном определении Суд признал законность проведенного следственного действия, аргументируя свою позицию тем, что

[1] Васюков В. Ф, Булыжкин А. В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2016. № 6. С. 4.

привлечения специалиста для изъятия мобильного телефона не требовалось ввиду того, что содержащаяся в телефоне информация в месте производства следственного действия не исследовалась и применения специальных знаний, которыми обладает специалист, не требовалось[1].

Однако УПК РФ никаких исключений из общего правила работы с электронными носителями информации не содержит, что не допускает самовольную трактовку рассматриваемой нормы.

Кроме того, по ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых осуществляется копирование информации с изымаемых электронных носителей информации на другие электронные носители, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации.

При этом следователь может отказать в удовлетворении ходатайства в случае, если:

– лицо, заявившее ходатайство, не обладает полномочиями на хранение и использование информации, хранившейся на носителях;

– информация может быть использована для совершения новых преступлений;

– копирование может повлечь за собой ее утрату или изменение (ст. 164.1 УК РФ).

Установление указанных условий в правоприменительной деятельности не всегда представляется возможным.

Во-первых, чтобы определить, является ли лицо законным владельцем информации, необходимо получить к ней доступ путем подключения электронного носителя к компьютеру или открытия конкретного файла и его просмотра, а эти действия могут послужить началом запуска программы по уничтожению информации.

Во-вторых, определить вероятность использования информации для совершения новых преступлений возможно только при глубоком анализе ее содержания, что тоже затруднительно осуществить в условиях проводимого следственного действия. Риск утраты или изменения информации при ее копировании все же имеется, но, как правило, основывается только на вероятных предположениях. К тому же субъективную следственную оценку, подкрепленную выводами привлеченного профильного специалиста, в рассматриваемом вопросе опровергнуть достаточно сложно. Поэтому в правоприменительной практике выяв-

[1] Апелляционное определение Верховного Суда Российской Федерации от 14 ноября 2019 г. № 205-АПУ19-37 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

лена тенденция многочисленных отказов в удовлетворении ходатайств о копировании информации, однако она не является безосновательной.

В правоприменительной практике немало случаев, когда собственники информации предоставляли в качестве накопителей для копирования информации USB Киллеры[1], что приводило к разрушению системы компьютера и утрате информации и доказательств. Кроме того, процесс копирования может занять продолжительное время, которым следователь не располагает. К тому же в соответствии со ст. 121 УПК РФ, в случаях, когда немедленное принятие решения по ходатайству, заявленному в ходе предварительного расследования, невозможно, оно должно быть разрешено не позднее трех суток со дня его заявления. Поэтому следователь после окончания следственного действия и изъятия информации может без риска осуществить ее копирование.

Несмотря на участие в следственном действии привлеченного специалиста, следователь не должен отдавать ему инициативу руководства следственным действием. Именно следователь как лицо, наделенное УПК РФ самостоятельностью в определении направления хода расследования, принятии решения о производстве следственных действий, должен осуществлять общее руководство его проведением. Весь процесс оказания помощи, для которой и привлекается специалист, должен быть осуществлен под контролем следователя, более того, все действия, проводимые специалистом, подлежат занесению в протокол соответствующего следственного действия.

Таким образом, тактико-криминалистические особенности проведения следственных действий определяются тактической ситуацией и соблюдением при их проведении общих рекомендаций, обеспечивающих законность, обоснованность, достоверность и допустимость полученных в ходе следственных действий доказательств.

Тактика проведения отдельных следственных действий будет рассмотрена в следующих параграфах.

Контрольные вопросы

1. Назовите основные тактико-криминалистические особенности проведения следственных действий при расследовании преступлений, совершенных с использованием ИТ-технологий.

2. Порядок организации работы при расследовании преступлений, совершенных с использованием информационных технологий.

---

[1] USB Killer – устройство, способное нанести большой ущерб системам, используя преимущества взаимодействия USB-накопителей и питания. Оно посылает высоковольтное питание на компьютер, к которому подключено, эффективно разрушая систему. USB Killer может посылать до 200 В постоянного тока в порт USB – смертельный удар для любой машины.

3. Что понимается под следственной ситуацией? Основные условия ее формирования, ее виды, присущие преступлениям, совершенным с использованием информационных технологий, и влияние на тактическую линию поведения следователя.

4. Понятие противодействия расследованию, основные методы его осуществления и меры его преодоления.

5. Специалист: понятие, условия его привлечения к следственным действиям и влияние его участия на результативность следственного действия.

6. Какими специальными знаниями должен обладать специалист, привлекаемый к следственным действиям, проводимым при расследовании преступлений, совершенных с использованием ИТТ?

7. Порядок привлечения специалиста.

§ 2. Тактика осмотра

Одним из первоначальных следственных действий при расследовании преступлений, совершенных с использованием ИТТ, является следственный осмотр. Статья 176 УПК РФ устанавливает основание производства следственного осмотра, в качестве которого определяет необходимость достижения цели по обнаружению следов преступления и выяснения других обстоятельств, имеющих значение для уголовного дела.

Цифровой след, как и любой другой вид информации, состоит из двух элементов:

1) материального носителя сведений, которым в данном случае выступает электромагнитное поле. Техническое устройство, в котором находится информация, рассматривается как вторичный материальный носитель информации и может иметь предметную форму с точными пространственными границами (наиболее часто исследуются компьютеры и их компоненты, микрокомпьютеры, встроенные в различные устройства, средства связи, сетевые технические средства, портативные системы видеонаблюдения; видеокамеры, фотоаппараты; диктофоны, органайзеры, навигационные устройства, съемные носители компьютерной информации), а может и не иметь предметной формы (при передаче информации по беспроводным каналам в компьютерных сетях);

2) информации, то есть сведений о каком-либо явлении объективной реальности, которая может оставаться в компьютерных и иных цифровых устройствах: в мобильных телефонах, диктофонах, фото- и видеокамерах и т. д.[1]

---

[1] Криминалистика : учебник : в 5 т. Т. 3. Криминалистическая техника / под ред. И. В. Александрова. М. : Юрайт, 2019. С. 216.

Уязвимость таких следов очевидна, поэтому очень важно уметь правильно работать с данной информацией, чтобы в последующем возможно было придать ей доказательственное значение. Необходимо соблюдать следующие общие рекомендации при работе с цифровыми следами преступления:

– применяемые методы обнаружения, фиксации и изъятия цифровых следов не должны приводить к их модификации;

– условия хранения цифровых следов должны исключать риски внешнего воздействия на них и уничтожения;

– признание их вещественными доказательствами должно быть осуществлено в кратчайший срок.

Тактическое решение о выборе необходимого для проведения вида следственного осмотра зависит от сформированной следственной ситуации, которая может быть конкретизирована в зависимости от наличия информации о потенциальном объекте осмотра (месте преступления, компьютерном устройстве).

Одной из распространенных следственных ситуаций, определяющих необходимость и возможность проведения осмотра места происшествия, является следственная ситуация, когда имеется информация только о наступивших последствиях от преступления. В этой связи местом происшествия является место, где наступили общественно опасные последствия, или иное место (место расположения транзитных носителей и т. п.).

Например, ФИО1, находясь в городе Казани Республики Татарстан и городе Волжск Республики Марий Эл, осознавая общественно опасный характер своих действий и желая наступления общественно опасных последствий в виде причинения имущественного ущерба, внеся заведомо ложные сведения в устройства самообслуживания (банкоматы), обманным путем похитил денежные средства в размере 75 000 рублей, принадлежащие ПАО «Сбербанк России»[1]. Одним из доказательств вины гр. ФИО1 являлись протоколы осмотров мест происшествий. Объектами осмотров выступали отделения банков, где находились банкоматы и устройства самообслуживания, с помощью которых были осуществлены денежные переводы.

Осмотр места происшествия, являясь первоначальным следственным действием, проводится для обнаружения, фиксации и изъятия следов преступления, восстановления обстановки происшествия, а также описания изъятых материальных объектов, имеющих отношение к уголовному делу, и установления отдельных обстоятельств, входящих в предмет доказывания (например, место совершения преступления).

---

[1] Приговор № 1-21/2024 1-737/2023 от 26 февраля 2024 г. по делу № 1-21/2024 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

Традиционно любое следственное действие, в том числе и осмотр места происшествия, делится на три этапа: подготовительный, рабочий и заключительный. Эффективность следственного действия зависит в том числе от качественной подготовки к его проведению.

На подготовительном этапе следователю необходимо оценить имеющиеся сведения о преступлении, подготовить необходимые технические средства поиска и фиксации следов преступления, криминалистические средства обнаружения, изъятия и упаковки обнаруженных следов, а также обеспечить участие обязательных участников осмотра места происшествия и определить необходимость привлечения факультативных – специалиста, понятых (ст. 168, ст. 170 УПК РФ).

Рабочий этап начинается с определения границ осмотра, выбора способа производства на его статической стадии. Динамическая стадия осмотра сводится к осуществлению деятельности по обнаружению, изъятию и фиксации следов преступления.

При осмотре помещения или отделения банка следователь должен соблюдать общие тактические приемы осмотра, к которым следует отнести:

– единство руководства осмотром со стороны следователя или лица, его производящего;

– объективность, всесторонность и полнота;

– своевременность;

– целеустремленность, планомерность и методичность;

– применение всевозможных криминалистических средств поиска и изъятия следов преступления;

– соблюдение криминалистических рекомендаций по работе со следами преступления.

Протокол осмотра места происшествия составляется с учетом требований, предусмотренных ст. ст. 166, 167, 180 УПК РФ, непосредственно в ходе проведения следственного действия или сразу после него, на заключительном этапе. Общие требования, предъявляемые к описанию объектов, сводятся к терминологической точности и единообразию хода описания от общего к частному, что обеспечит правильное понимание зафиксированных сведений об обнаруженных объектах, а описанные признаки позволят индивидуализировать фиксируемый объект.

Кроме того, в соответствии со ст. 164 УПК РФ, следователь может применять и технические средства обнаружения, фиксации и изъятия следов преступления и вещественных доказательств, а также фиксации хода и результатов осмотра места происшествия.

В рассматриваемой следственной ситуации осмотр помещения проводится с соблюдением общих тактических правил осмотра от общего к частному, снаружи внутрь, сверху вниз.

В качестве объекта осмотра могут выступать банкоматы или терминалы, располагающиеся как в отделениях банков, так и в иных помещениях.

Банкомат имеет принадлежность к соответствующему банку, о чем свидетельствуют информационные указатели на устройстве, идентификационный номер, и всегда находится на прямой связи с банком. Банкомат имеет кнопочную или сенсорную клавиатуру и отделения для выдачи и/или приема денег. В корпус банкомата встроен компьютер с определенной операционной системой и дополнительными программами. Использование банкомата возможно при наличии банковской карты, которая помещается в него или размещается на настроенный бесконтактный модуль (passpay – пасспэй) для считывания информации о держателе карты, посредством использования мобильного телефона или QR-кода. Кроме того, зачастую банкоматы оборудованы камерами видеонаблюдения, и в ходе осмотра места происшествия возможно осуществить копирование соответствующей видеозаписи.

Терминал – это устройство, предназначенное для выполнения определенных задач, таких как оплата услуг или товаров, предоставление информации, выдача билетов, осуществление различных платежей, переводов. В этом случае пользователь идентифицирует себя путем ввода сведений о плательщике или информации о держателе используемой банковской карты, если функционал терминала позволяет ее использовать.

Таким образом, при осмотре банкомата и терминала следует отразить:

– место нахождения устройства;
– принадлежность к организации;
– идентификационный номер устройства;
– наличие камеры видеонаблюдения и изъятие видеозаписей.

Несмотря на то, что в ходе осмотра места происшествия вышеперечисленную информацию возможно установить на самом устройстве, в банке необходимо запросить сведения о банкомате, размещенном по соответствующему адресу, поскольку нередки случаи, когда указанные идентификационные данные на банкомате не соответствуют действительности. Кроме того, необходимо запросить и иную интересующую информацию об операциях, проведенных с использованием соответствующего устройства, у организации-владельца. При осмотре места происшествия следует обращать внимание и на урны, расположенные возле банкоматов, в которых можно обнаружить чеки о соответствующих операциях.

Менее распространенной следственной ситуацией является ситуация, когда имеется информация о преступлении, в частности о месте совершения преступления, в котором возможно обнаружить электронные носители информации, следы преступления, в том числе цифровые.

Так, ФИО1, являясь директором ООО «УК «СЖК» и в соответствии с Уставом ООО «УК «СЖК» единоличным исполнительным органом

Общества, осуществляя руководство текущей деятельностью Общества, представляя его интересы и совершая сделки от имени Общества, издавая приказы и давая указания, обязательные для исполнения всеми работниками Общества, имея право первой подписи на финансовых документах, умышленно, незаконно использовал объекты авторского права в крупном размере, используя свое служебное положение. Директор ООО «УК «СЖК», осознавая незаконный, противоправный характер своих действий и зная, что у ООО «УК «СЖК» отсутствуют лицензионные соглашения с ООО «1С» и ООО «1С-Софт» на право использования в деятельности ООО «УК «СЖК» программ для электронно-вычислительных машин (далее – ЭВМ), из корыстных побуждений, незаконно хранил в памяти ЭВМ и использовал в текущей деятельности Общества следующие нелицензионные программы для ЭВМ: «1С: Предприятие 7.7 Для SQL. Комплексная поставка» – 2 экземпляра, «1С: Предприятие 7.7 Сетевая версия. Комплексная поставка» – 3 экземпляра, «1С: Предприятие 7.7 ПРОФ. Комплексная поставка» – 1 экземпляр, «1С: Предприятие 7.7 Управление распределенными информационными базами» – 2 экземпляра, «1С: Предприятие 8.3 Технологическая поставка» – 1 экземпляр, «1С: Предприятие 8. Клиентская лицензия на 10 рабочих мест» – 1 экземпляр.

Вышеуказанное программное обеспечение ФИО1 умышленно, незаконно использовал при осуществлении финансово-хозяйственной деятельности ООО «УК «СЖК до момента, когда сотрудники полиции в ходе осмотра места происшествия в помещении ООО «УК «СЖК», расположенном по адресу: <адрес>, изъяли пять системных блоков, используемых в деятельности ООО «УК «СЖК», которые были признаны вещественными доказательствами[1].

В данном случае в ходе осмотра места происшествия поиску, фиксации и изъятию подлежат следующие объекты:

– компьютерные устройства;

– внешние электронные носители (диски, в том числе жесткие, флеш-карты и т. п.).

При этом к числу компьютерных устройств могут быть отнесены любые электронные устройства, произведенные или переделанные промышленным либо кустарным способом и способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов: персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами

[1] Приговор № 1-264/2023 от 6 октября 2023 г. по делу № 1-264/2023 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека[1].

В целях обнаружения, фиксации и изъятия компьютерных устройств следователь должен соблюдать тактические рекомендации, обеспечивающие сохранность цифровых следов. Для этого до начала осмотра необходимо запретить работу на компьютерных устройствах. Далее необходимо выяснить общие сведения об устройствах и местах их расположения. К общим сведениям следует отнести информацию об организации компьютерной инфраструктуры, видах, моделях, комплектации, маркировочных обозначениях, инвентаризационных и серийных номерах, а также возможных индивидуальных признаках таких устройств (наличие механических повреждений, наклеек и др.).

К сведениям об организации компьютерной инфраструктуры относятся:

– расположение устройств, топология сети;
– данные о системном администрировании;
– домен, права пользователя на рабочих станциях;
– технология, схема осуществления доступа в Интернет;
– провайдер услуг, хостинг-провайдер, регистратор доменного имени;
– межсетевой экран прокси-сервера;
– внешние IP-адреса компании.

Необходимо проверить, подключены ли компьютеры к элементам питания, в каком состоянии на момент осмотра находятся устройства (вкл./выкл.) и подключено ли к ним внешнее оборудование (клавиатура, мышь, колонки, флеш-накопители, модемы и т. п.). Подключение устройств к проводной или беспроводной сети Интернет, а также необходимость отключения персонального компьютера от сети Интернет оценивается специалистом в каждом конкретном случае.

Необходимо помнить, что в таких устройствах источники информации могут быть как энергонезависимыми, так и энергозависимыми.

К энергонезависимым источникам относятся:

– отдельные файлы и каталоги;
– журналы систем протоколирования;
– логи-файлы (текстовый файл, куда автоматически записывается важная информация о работе системы или программы) сетевого оборудования, DLP-система – специализированное программное обеспечение, предназначенное для защиты компании от утечек информации;
– логи-файлы провайдера;
– данные интернет-сервисов;

---

[1] Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/.

– содержимое оптических дисков и накопителей на основе флеш-памяти;

– накопитель на жестких магнитных дисках (НЖМД);

– рабочие станции, серверы.

При этом специалист осуществляет копирование – создание образа (полного, частичного или логического) этих систем.

К энергозависимым источникам относятся:

– оперативная память;

– сетевой трафик;

– список открытых файлов со сведениями;

– временные журналы регистрации событий;

– hiberfil.sys – скрытые системные файлы, которые создаются автоматически в том случае, если устройство переходит в режим гибернации;

– pagefile.sys – это файл подкачки операционной системы Windows. При нехватке оперативной памяти Windows резервирует определенное место на жестком диске и использует его для увеличения своих возможностей;

– swapfile.sys является аналогом файла подкачки pagefile.sys, но используется в качестве виртуальной памяти для временного хранения данных современных приложений.

Если компьютер включен, то не следует сразу отключать его от источника питания, поскольку информация о процессе работы будет уничтожена. Специалист осуществляет изъятие дампа оперативной памяти с обнаруженного устройства, поскольку оперативная память – это энергозависимая часть компьютерной памяти, позволяющая сохранить информацию о выполняемых программах и промежуточных данных, обрабатываемых процессором ровно до того момента, пока источник питания не будет отключен.

Изъятие дампа оперативной памяти позволит получить следующую информацию:

– перечень запущенных процессов;

– сведения о сетевых соединениях;

– пароли;

– расшифрованные файлы;

– ключи шифрования;

– буфер обмена;

– переписка;

– вредоносные коды.

При изъятии дампа сетевого трафика возможно получить сведения:

– о программном элементе браузера, который обозначает пользователя (User agent), – эта информация хранится в файле и позволяет идентифицировать пользователя;

– о производителе сетевых карт;

– о модели атаки;
– о соединениях и передаваемых файлах;
– об участвующих устройствах.

Информацию о запущенных программах, процессах и используемых ими ресурсах возможно просмотреть через вспомогательную компьютерную программу (утилита) – диспетчер задач (комбинация клавиш Ctrl+Shift+Esc или Ctrl+Alt+Delete). Следует изучить и проанализировать каждую запущенную программу и оценить важность и ценность обнаруженной кратковременно существующей информации, поскольку ее копирование с оперативного запоминающего устройства может повлечь за собой изменение информации, хранящейся на компьютере.

В ходе осмотра возможно осуществить и копирование информации, хранящейся на НЖМД осматриваемого компьютера. Для этого специалист может физически извлечь НЖМД из выключенного осматриваемого компьютера, подключить его к компьютеру с соответствующим программным обеспечением либо к аппаратному автономному устройству и осуществить копирование имеющимися средствами (либо же, подключив дополнительный НЖМД, скопировать на него информацию). Выбор способа определяет специалист, исходя из имеющихся в его распоряжении программно-аппаратных средств.

Изъятие дампа памяти, сетевого трафика, НЖМД должно осуществляться на запоминающие устройства, имеющие функцию блокировки от записи, в целях обеспечения сохранности и исключения возможности доступа к содержащейся на них информации. Кроме того, следует помнить, что любые действия с компьютером могут быть осуществлены при условии исключения риска запуска автоматизированных процессов уничтожения информации.

Все выполненные с компьютером действия подлежат фиксации в протоколе следственного действия осмотра места происшествия. Чтобы исключить в дальнейшем вопросы относимости и допустимости полученных в ходе осмотра места происшествия доказательств, необходимо в протоколе осмотра места происшествия осуществить надлежащую фиксацию обнаруженных объектов и следов, а также всех проводимых с ними действий по изъятию.

Таким образом, при обнаружении компьютера в протоколе осмотра места происшествия следует указать:

– вид, марку, комплектность, наличие проводов питания, правильность их подключения, расположение устройства в сети подключенных устройств, номер (серийный, инвентарный или учетный), цвет и индивидуальные признаки;

– состояние на момент осмотра (выключено или включено);

– наличие проводного или беспроводного подключения к сети Интернет;

– наличие подключенных флеш-накопителей, их вид, объем и индивидуальные признаки;

– наличие следов преступления (материальных, цифровых).

Если на момент осмотра компьютер находится в рабочем состоянии, необходимо детально описать:

– расположение его рабочих механизмов и изображение на его видеоконтрольном устройстве (экране, мониторе, дисплее);

– какие файлы, интернет-страницы открыты, при этом можно просмотреть и описать последние открытые документы и историю браузера;

– основные действия, производимые специалистом при осмотре компьютера (порядок корректного приостановления работы и закрытия исполняемой операции или программы, выключения компьютера, отключения от источника электропитания, разъединения (или соединения) каомпьютера, отсоединения проводов, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т. п.)[1];

– способ изъятия и упаковки.

Сам фактический процесс изъятия требует соблюдения требований по работе с компьютерными устройствами, направленных на сохранение хранящейся на данных устройствах информации. Так, при изъятии серверов, системных блоков рабочих станций, ноутбуков (в случае, если они находятся во включенном состоянии) следует произвести корректный выход из системы для предотвращения потери данных, т. е. произвести корректное выключение объектов (см. рис. 2).

В этом случае закрываются все открытые программы и файлы, стираются временные файлы, а если есть вредоносные программы, например

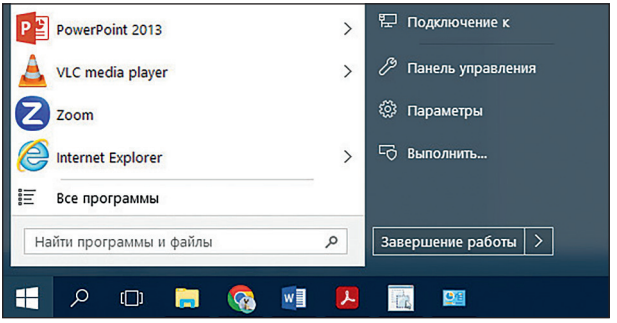


Рис. 2. Выключение персонального компьютера, работающего под управлением ОС семейства «Windows»

[1] Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учеб.-метод. пособие / Э. Д. Нугаева, С. Р. Низаева, В. Р. Гайнельзянова и др. Уфа : Уфимский юрид. ин-т МВД России, 2023. С. 42.

троян или руткит, то при активации команды завершения работы они могут запустить функцию уничтожения следов своего присутствия.

Далее все изъятые устройства перед упаковкой должны быть опечатаны.

При изъятии системного блока необходимо:

– опечатать разъем электрического питания (как правило, он находится на задней панели);

– опечатать боковые стенки системного блока (так, чтобы невозможно было осуществить доступ к его содержимому);

– опечатать устройства для работы с оптическими дисками, flash-накопителями, накопителями на гибких магнитных дисках (см. рис. 3)[1].

Ноутбуки и нетбуки опечатываются в закрытом положении таким образом, чтобы невозможно было открыть крышку ноутбука и включить его, не нарушив целостность опечатывающей бирки (см. рис. 4).

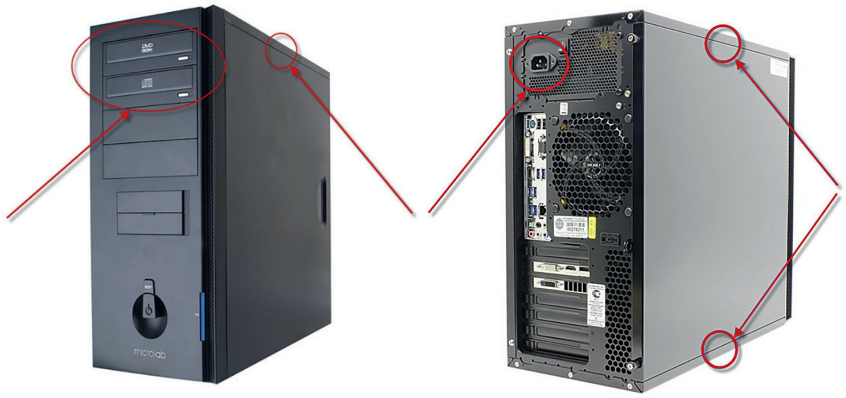


Рис. 3. Места опечатывания системного блока

Рис. 4. Место опечатывания ноутбука

[1] Рис. 3–15 предоставлены ЭКЦ ГУ МВД России по Алтайскому краю.

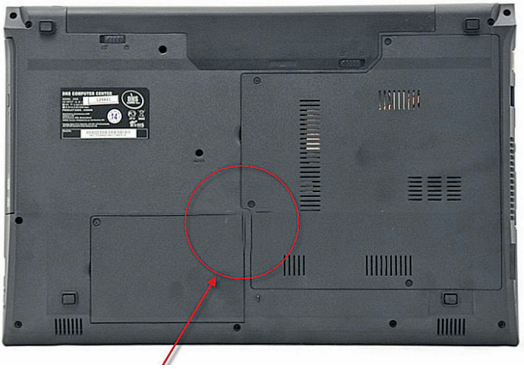


Рис. 5. Место опечатывания ноутбука

Также необходимо опечатать отсеки для накопителей информации (см. рис. 5).

В соответствии с приказом МВД России от 29 июня 2005 г. № 511[1], упаковка объектов должна содержать пояснительные надписи и исключать возможность доступа к содержимому без ее повреждения, обеспечивать сохранность. Таким образом, характер и вид упаковочного материала выбирается с учетом размерных, весовых характеристик изымаемого объекта.

Наиболее оптимальный способ упаковки – коробка, пакет, мешок (см. рис. 6, 7).

В случае большого количества системных блоков допускается изъятие не самих системных блоков, а накопителей информации, установленных в них. При этом необходимо зафиксировать в протоколе, из какого системного блока изъят «жесткий диск», и его маркировочные обозначения (марка, модель, серийный номер, заявленная емкость) (см. рис. 8).

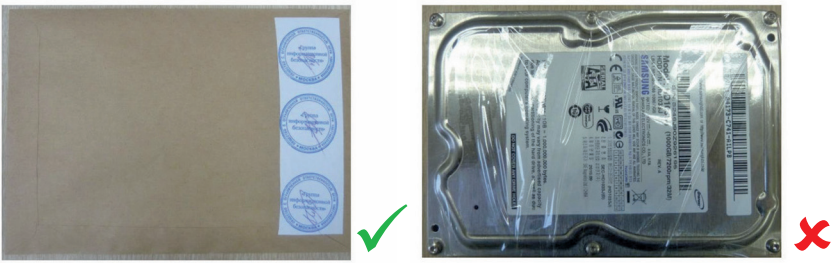
Наиболее подходящим упаковочным материалом для накопителей на жестких магнитных дисках является:

– картонная коробка (клапаны коробки опечатываются печатью);

– полимерный пакет (горловина пакета стягивается нитью, концы нити опечатываются печатью).

---

[1] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с «Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации») : приказ МВД России от 29 июня 2005 г. № 511 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_55315/.



упаковка НЖМД
без нарушений

упаковка НЖМД
с нарушениями

Рис. 6. Пример упаковки НЖМД

Рис. 7. Пример упаковки системного блока

Рис. 8. Индивидуализирующие признаки накопителя
на жестких магнитных дисках

Очень важно обеспечить надлежащие условия транспортировки и хранения изъятых устройств, ограничив их от воздействия вибрации или иных механических повреждений, а также высокой температуры, влажности для сохранения работоспособности.

Мобильные телефоны также относятся к компьютерным устройствам и активно используются в преступной деятельности.

Так, по делу № 2-106/2024 мобильные телефоны и информация, содержащаяся на них, были признаны доказательствами в незаконном производстве наркотических средств, совершенном группой лиц по предварительному сговору, в особо крупном размере, незаконные приобретение, хранение прекурсоров наркотических средств, совершенные в особо крупном размере. Группа лиц, вступив в сговор, совместно незаконно производили наркотических средств в особо крупном размере с целью их дальнейшего сбыта, и на незаконно приобретали и хранили прекурсоры наркотических средств в особо крупном размере, для использования их при серийном производстве наркотического средства а-пирролидиновалерофенон (синоним а-PVP), являющегося производным наркотического средства – N- метилэфедрона[1].

Поэтому мобильные телефоны и смартфоны подлежат обязательному изъятию с последующим изучением хранящейся на них информации. В повседневной жизни понятия мобильный телефон и смартфон употребляются как тождественные, постановление Пленума Верховного Суда Российской Федерации № 37 разделяет их. На самом деле смартфон представляет собой более функциональное устройство, сочетающее в себе функции мобильного компьютера, позволяющие использовать его для разнообразных задач, в первую очередь доступа к высокоскоростной сети Интернет, и имеющее операционные системы и большой объем встроенной памяти. Мобильные же телефоны представляют собой более простые устройства для связи, в некоторых случаях не имеющие возможности выхода в Интернет, но тем не менее и они отнесены к компьютерным устройствам, поскольку позволяют использовать сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен информацией (передачу сообщений) между компьютерными устройствами. В данном пособии мы не будем разделять эти понятия. Мобильные телефоны являются устройствами сотовой связи, выполняя функции от базовых (средство связи и записной книжки) до расширенных (функции

[1] Приговор № 2-106/2024 от 26 августа 2024 г. по делу № 2-106/2024 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

компьютера), и используются каждым человеком в современном мире. Они содержат микропроцессор, постоянное запоминающее устройство (ROM), оперативное запоминающее устройство (RAM), аналого-цифровой преобразователь, микрофон и громкоговоритель, ряд аппаратных ключей и интерфейсов и поэтому, безусловно, являются носителями цифровых следов и представляют криминалистический интерес. Оперативный и криминалистический интерес представляет хранящаяся на таких объектах информация о контактах, смс-сообщениях, записях паролей, фото-, видеозаписях и т. д. Кроме того, мобильное устройство содержит сведения, хранящиеся в облачных сервисах, удаленных серверах, мессенджерах и социальных сетях.

Удаленный контент, сложные системы блокировки телефонов, барьеры шифрования, необходимость глубокого анализа на физическом уровне, на уровне файловой системы и аналогичные сложности для просмотра данных телефона не позволяют провести осмотр содержимого телефона на месте его обнаружения, к тому же эта работа может занять продолжительный период времени. Поэтому изучение информационного содержания телефона происходит, как правило, в рамках самостоятельного следственного осмотра предметов и документов после назначенной и проведенной экспертизы, объектом которой выступает мобильный телефон, и после его разблокировки. В случае обнаружения телефона на месте происшествия следователь ограничивается внешним визуальным его осмотром, указывая в протоколе вид, модель, внешний вид, состояние, наличие на корпусе кнопок управления и их расположение, а также индивидуальные признаки, например наличие чехла, брелоков.

Следует помнить, что на корпусе телефона могут сохраниться материальные следы отображения (следы пальцев рук), поэтому, обнаружив телефон, необходимо осуществить их поиск и изъятие. Однако следователь, решая эту задачу, должен расставить приоритеты между возможностью обнаружить материальные следы и необходимостью сохранить криминалистически значимую информацию. Кроме того, химические методы обнаружения следов пальцев рук, например с использованием нингидрина, цианоакрилата, могут привести телефон в негодность[1].

При изъятии мобильного устройства должна быть обеспечена сохранность информации, хранящейся на нем, поэтому мобильные устройства (телефоны, планшеты) необходимо отключить от сетей Wi-Fi, GPS, NFC, Bluetooth и перевести в автономный режим, т. е. режим полета, особенно если производится упаковка устройств во включенном состоянии, так как

[1] Прокофьев А. А. Участие специалиста при изъятии цифровых мобильных устройств // Актуальные проблемы криминалистики и судебной экспертизы : мат-лы междунар. науч.-практ. конф. Иркутск : Восточно-Сибирский институт МВД России, 2021. С. 163–166.

к включенным мобильным устройствам остается возможность дистанционного подключения через Интернет и удаления информации. В практике известны случаи, когда при изъятии мобильного телефона без участия специалиста оперуполномоченные для получения оперативно значимой информации временно сняли автономный режим, произошло удаленное подключение к устройству и удаление учетной записи – и в результате на компьютерную экспертизу устройство поступило в деактивированном виде.

Вот почему очень важно незамедлительно перевести устройство в автономный режим работы. При этом не рекомендуется полностью выключать устройство, вынимать аккумулятор (хотя телефоны типа смартфонов имеют встроенный аккумулятор), а при необходимости следует осуществлять подзарядку. Также рекомендуется изъять и кабели к мобильным устройствам.

Следует решить вопрос об изъятии физического образа с телефона. Возможность его изъятия в ходе осмотра места происшествия определяется специалистом и зависит от наличия информации о паролях и технической возможности. Изъятая информация копируется на электронный носитель для дальнейшего осмотра и изучения. Сам изъятый мобильный телефон упаковывают в непрозрачный пакет в целях предотвращения доступа к дисплею.

Поиск криминалистически значимой информации и аналитическая работа следователя с ней начинается в ходе осмотра предметов и документов. Функциональная сложность и защищенность компьютерных устройств не позволяет сделать это в ходе осмотра места происшествия. Все изъятые в ходе осмотра места происшествия компьютерные устройства подлежат осмотру. Следователь и участвующий специалист должны уметь выявлять, расшифровывать и сохранять полученную информацию. Возможные неосторожные манипуляции с осматриваемым устройством могут повлечь безвозвратное удаление криминалистически значимой информации, в связи с чем категорически запрещается переустанавливать оперативную систему, удалять детекты антивируса, а также вносить изменения в состояние систем.

Осмотр компьютера необходимо начать с выяснения характеристики операционной системы, установленной на компьютере. Выяснить эту информацию возможно, открыв проводник, нажав на значке «компьютер» правой кнопкой мыши и выбрав свойства. Сетевые (активные и неактивные) интерфейсы необходимо просмотреть, используя проводник: Пуск – Панель управления – Сеть и Интернет – Центр управления сетями и общим доступом – Изменение параметров адаптера. Состояние активных интерфейсов (длительность подключения, объем переданных и полученных данных) проверяется путем вызова меню правой кнопкой мыши. Текущее подключение выясняется путем нажатия кнопки

«Сведения» – в данном разделе сохраняется информация о текущем IP-адресе компьютера; о типе распределения адресов в данном сегменте исследуемой локальной сети; об IP-адресах DHCP-, DNS-серверов.

Поиск информации определенного содержания (ключевых слов в текстовых файлах и информационных базах данных, файлов с определенным расширением) на компьютерах, работающих под управлением операционной системы семейства «Windows», целесообразно проводить, используя встроенные средства поиска сведений о работе пользователя в сети Интернет (см. рис. 9, 10) и переписки посредством сети Интернет (см. рис. 11).

Также для поиска информации можно использовать так называемые файловые менеджеры, среди которых наиболее популярны Total Commander, Speed Commander, oMega Commander, Unreal Commander, Free Commander, Double Commander, Multi Commander, XYplorer. Функциональным является Total Commander: удобный интерфейс, возможность отображения скрытых файлов (см. рис. 12), сортировки файлов по расширению, поиска файлов по определенным критериям.

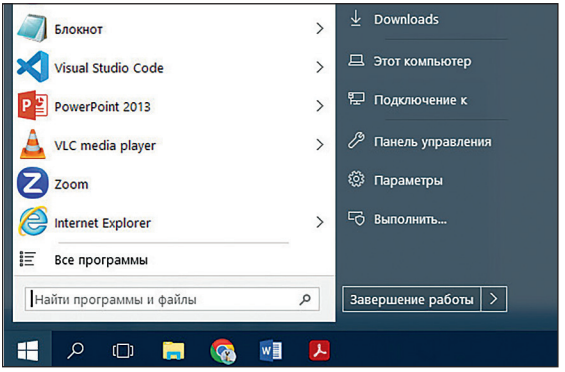


Рис. 9. Стандартные средства поиска ОС «Windows 10»

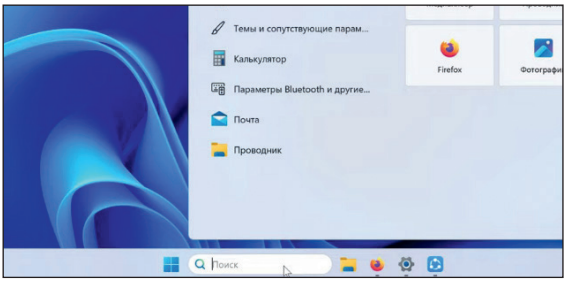


Рис. 10. Стандартные средства поиска ОС «Windows 11»

Рис. 11. Ярлыки наиболее популярных программных продуктов, предназначенных для работы с электронной почтой

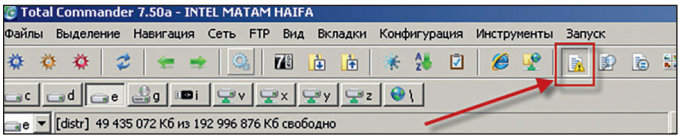


Рис. 12. Рабочее окно программы Total Commander. Отображение скрытых элементов

Для запуска функции поиска файлов необходимо использовать комбинацию клавиш «Alt+F7» (рис. 13–15).

Каждый этап поиска и обнаруженные в его результате системные папки, файлы описываются в протоколе, а в качестве дополнительного средства фиксации может быть использована функция Print Screen (снимок экрана). Однако в правоприменительной деятельности сложилась негативная практика, когда следователь изготавливает только скриншоты экрана, не описывая в протоколе осмотра путь обнаружения криминалистически значимой и доказательственной информации. Следует помнить, что иллюстрации экрана – это лишь приложение к протоколу осмотра, а доказательством признается именно протокол следственного действия. Обнаруженная информация подлежит оценке с точки зрения содержания и относимости к преступлению (нецелесообразно описывать всю без исключения обнаруженную информацию).

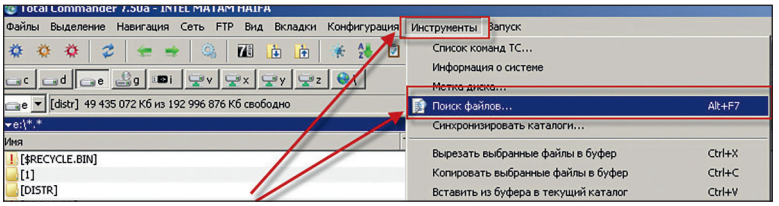


Рис. 13. Рабочее окно программы Total Commander. Запуск функции «Поиск файлов»

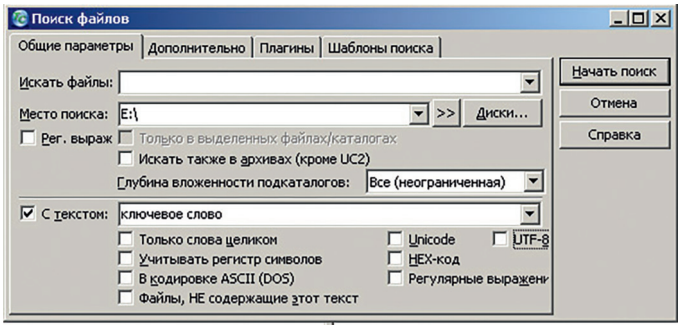


Рис. 14. Рабочее окно программы Total Commander.
Поиск файлов по ключевому слову

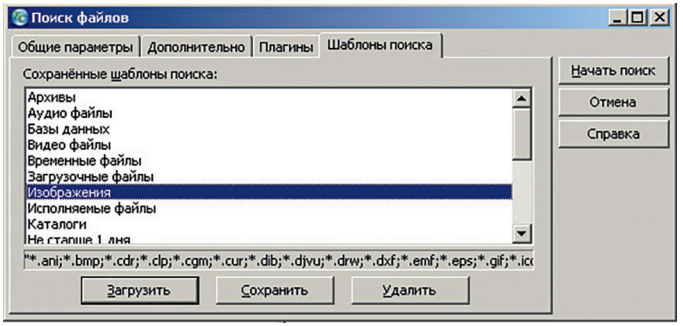


Рисунок 15. Рабочее окно программы Total Commander.
Поиск файлов по расширению

Например, в ходе осмотра DVD-R-диска, на который было осуществлено копирование информации, установлено, что на данном диске содержится папка «восстановленные файлы», включающая папки: архив, графика, изображение, документ. Папка «история» содержит XL-файлы: загруженные файлы, ссылки, пароли, ссылки. В папке «документ» есть папка, содержащая PDF-файлы. При открытии файла извлечен документ – полис ОСАГО о страховании владельца транспортного средства П. После осмотра диск упакован. Данный DVD-R-диск признан вещественным доказательством[1].

Более того, при работе с компьютерами могут быть применены специализированные инструменты, которые помогают извлекать удаленную информацию, анализировать и сохранять доказательства.

[1] Материалы уголовного дела № 1-142/2022 // Архив Советского районного суда г. Самары за 2022 год.

К ним относятся:

1. Разработчик МКО «Системы»:

а) программный продукт «Мобильный Криминалист Эксперт» – многофункциональный инструмент для высокоскоростной и эффективной работы с данными из мобильных устройств, дронов, облачных сервисов и персональных компьютеров;

б) программный продукт «Мобильный Криминалист Десктоп» – инструмент для извлечения информации с персонального компьютера.

2. Разработчик Elcomsoft (Россия):

а) Elcomsoft iOS Forensic Toolkit – для проведения криминалистического анализа устройств, работающих под управлением Apple iOS;

б) Elcomsoft Phone Breaker – для извлечения и расшифровки данных из резервных копий устройств iOS, Windows Phone и BlackBerry и соответствующих облачных сервисов;

в) Elcomsoft Phone Viewer – для просмотра информации, извлеченной из резервных копий устройств под управлением iOS, облачных сервисов iCloud и Microsoft;

г) Elcomsoft Cloud Explorer – доступ к информации из Google Account;

д) Elcomsoft Explorer for WhatsApp – извлечение, просмотр и анализ истории сообщений пользователей WhatsApp.

3. Разработчик ACELab – программно-аппаратный комплекс PC3000 Mobile – извлечение данных из мобильных устройств.

4. Разработчик «Лан-проект» – аппаратно-программный комплекс исследования и анализа мобильных устройств АПК ИАМУ. Все типы АПК ИАМУ могут комплектоваться: Мобильный Криминалист Эксперт, iOS Forensic Toolkit, ПАК PC3000 Mobile, однако не все они имеются в распоряжении экспертных подразделений.

Следует отметить, что ввиду санкций многие производители перестали осуществлять обслуживание программно-аппаратных комплексов, используемых для работы с компьютерными устройствами, например UFED Touch производства израильской компании Cellebrite1 (UFED – Universal forensic extraction device). Он представляет собой устройство, снабженное сенсорным экраном, операционной системой и набором программных модулей, которые позволяют осуществлять физическое и логическое копирование данных устройства, извлечение системных файлов и паролей, сведений о мобильном устройстве.

Если осмотр компьютера проводится по преступлению в сфере компьютерной информации, то после резервного копирования файлов специалист проводит его тестирование с целью обнаружения вредоносных программ посредством антивирусного программного обеспечения. В случае обнаружения вредоносного программного обеспечения этот факт необходимо зафиксировать в протоколе. Зараженные файлы в последующем будут исследованы на предмет установления вида про-

граммного обеспечения, последствий от его воздействия, данных о его создании.

Осмотр содержания мобильного телефона начинается с указания его общих характеристик, которые уже были отражены в протоколе осмотра места происшествия и ранее в пособии были обозначены.

Далее необходимо в ходе осмотра узнать IMEI и EID путем нажатия комбинации (*#06#). IMEI представляет собой международный идентификатор мобильного оборудования в виде уникального кода из 15-ти цифр, который присваивается каждому мобильному телефону и смартфону на этапе производства и служит для распознавания устройства в сети. Современные мобильные устройства, позволяющие использовать две сим-карты, имеют два кода IMEI. EID – уникальный идентификатор eSIM на устройстве. Мобильные операторы используют EID для скачивания профилей SIM-карты для подключения к мобильным сетям.

ЭКЦ МВД России совместно со Следственным департаментом МВД России и ГУНК МВД России выработаны рекомендации[1] по алгоритму действий при работе с мобильным телефоном, соблюдение которых позволит получить доступ и сохранить хранящуюся в нем информацию.

Анализ данных рекомендаций и практики расследования преступлений рассматриваемой направленности позволил сформировать следующий алгоритм действий:

1. Установить пароль доступа к устройству и отразить его в протоколе. Следует отметить, что в некоторых устройствах может быть включена функция автозапоминания паролей для различных аккаунтов (например, в системе IOS: настройки – пароли – параметры паролей – автозапоминание паролей), а также указан разрешенный метод заполнения. Установленный пароль или информацию о предполагаемом пароле необходимо передать в экспертные подразделения при направлении телефона на экспертизу. Не стоит спешить сбрасывать код-пароль, поскольку эти действия могут повлечь за собой отключение устройства от сервисов и служб, связанных с облачным хранилищем, транзакций систем мобильных платежей и иных данных приложений, требующих наличия кода блокировки, и привести к утере криминалистической и доказательственной информации.

2. Установить наличие на устройстве дополнительных рабочих пространств, т. е. дополнительных рабочих областей, куда могут быть добавлены различные программы, мессенджеры и прочие сервисы.

---

[1] Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров. Москва : ЭКЦ МВД России, Следственный департамент МВД России, ГУНК МВД России, 2020. С. 17.

3. Определить наличие установленных программ-мессенджеров для обмена текстовыми сообщениями, аудиозаписями и сервисов, находящихся на момент осмотра во включенном состоянии; проанализировать их содержание и зафиксировать информацию в протоколе, создать скриншоты экрана, которые в последующем подлежат осмотру.

Так, одним из доказательств по уголовному делу № 1-43/2023 Хангаласским районным судом Республики Саха (Якутия) был признан протокол осмотра документов от 25 июня 2021 г., в котором осмотрены распечатанные скриншоты с экрана телефона подсудимого Л.: на 1 листе имеется изображение экрана телефона с перепиской «<данные изъяты> Итого: 109 250,00 руб.». На третьем листе имеется изображение экрана телефона с перепиской. Указанные скриншоты признаны и приобщены к уголовному делу в качестве вещественных доказательств с приложенной фототаблицей[1].

Отключить в настройках функцию автоматического удаления сообщений. При обнаружении защищенных паролем сервисов и мессенджеров установить пароль и внести его в протокол. При этом следует обращать внимание на все иконки программ, а не только на привычные логотипы мессенджеров, поскольку в практике известны случаи маскировки программ для общения под иконки иных программ, например калькулятор.

5. Проверить наличие закладок, т. е. сохраненных ссылок на интернет-сайты для быстроты пользования, и историю посещаемых интернет-ресурсов. Полученные сведения отразить в протоколе.

6. Осуществить проверку устройств на наличие программ-шпионов. В случае обнаружения принять меры для их отключения.

7. Осмотреть содержание программ, фиксирующих заметки пользователя, календарей, ежедневников и сервиса «документы» на наличие в них логинов и паролей, а также другой значимой информации.

8. Проверить хранилище графических изображений («галерея») на предмет определения круга общения, наличия фотографий с мест «закладок» и тайников, а также иной информации, способствующей изобличению задержанного в противоправной деятельности.

При осмотре мобильного телефона в протоколе осмотра предметов и документов следует указать:

– вид устройства, марку и модель, размеры, цвет, характеристику клавиатуры или кнопок (при наличии), фоновый рисунок, информацию, отображаемую на дисплее, наличие повреждений, украшений или наклеек;

---

[1] Приговор Хангаласского районного суда Республики Саха (Якутия) по делу № 1-43/2023 // Хангаласский районный суд Республики Саха (Якутия) : сайт. URL: https://pokrovsk--jak.sudrf.ru/modules.php?name=sud_delo&name_op=doc&number=1698535619&delo_id=1540006&case_type=0&new=0&text_number=1&srv_num=1.

– IMEI-код устройства;

– абонентский номер используемой SIM-карты, идентифицирующий возможного пользователя;

– информацию о входящих, исходящих и пропущенных соединениях, хранящуюся в памяти телефона. Такую информацию возможно получить и в рамках ст. 186.1 УПК РФ путем направления в организацию, осуществляющую услуги связи, копии обязательного для исполнения постановления суда о разрешении получения информации о соединениях между абонентами и (или) абонентскими устройствами;

– информацию об учетной записи владельца осматриваемого телефона в разделе настройки (имя, номера телефонов, e-mail) и об иных устройствах, активированных под этой учетной записью;

– информацию «Об этом устройстве»: имя, название номер, и серийный номер модели, сохраненные Wi-Fi данные устройства, SEID – идентификатор для регистрации устройства при осуществлении бесконтактных платежей, EID – встроенный идентификационный документ SIM-карты, сведения о физической SIM-карте и цифровой e-Sim-карте;

– данные о MAC-адресе устройства («Настройки» – «Основные» – «Об этом устройстве» – «Адрес WI-FI»), с которого происходила раздача, и выделенный IP-адрес;

– в приложениях, мессенджерах данные об аккаунте и привязанных банковских картах, в том числе виртуальных электронных кошельках[1].

В ходе осмотра мобильного телефона или компьютера могут быть обнаружены сведения об истории посещения веб-сайтов, социальных страницах пользователя, электронной почте, различных сервисах обмена мгновенными сообщениями и голосовой связи (WhatsApp, Viber, Telegram).

Социальные сети информационно-телекоммуникационной сети Интернет и сервисы обмена мгновенными сообщениями и голосовой связи являются самым простым, быстрым и доступным способом передачи информации в информационно-телекоммуникационной среде. Доступность, распространенность и простота использования делают их привлекательными не только для общения в рамках преступной деятельности, но и для реализации преступного умысла.

Так, ФИО6, находясь по адресу своего проживания, используя личный мобильный телефон марки и модели «Apple iPhone 7», имеющий возможность выхода в Интернет, с установленной в нем sim-картой с абонентским номером +№, имея доступ к аккаунту в интернет-сервисе «Авито», зарегистрированному на неустановленное следствием лицо,

[1] Нугаева Э. Д. Особенности производства осмотра места происшествия по преступлениям, связанным с незаконным сбытом наркотических средств и психотропных веществ, совершенным дистанционным способом // Экспертная практика. 2023. № 2 (94). С. 38.

имея преступный умысел, непосредственно направленный на хищение чужого имущества путем обмана, с причинением значительного ущерба гражданину, а именно на хищение денежных средств, представившись вымышленным женским именем, разместил в вышеуказанном интернет-сервисе «Авито» объявление о продаже мобильного телефона марки и модели «Apple iPhone XR», указав цену 15 000 рублей.

ФИО2, не подозревая о преступных намерениях ранее ей незнакомого ФИО6, вступила с ним в электронную переписку, в ходе которой высказала желание приобрести мобильный телефон марки и модели «Apple iPhone XR» за 15 000 рублей, а ФИО6 в свою очередь с целью реализации своего преступного умысла сообщил ей о необходимости внесения предоплаты в размере 6 500 рублей на принадлежащий ему электронный кошелек №, на что ФИО2, убежденная в правдивости намерений «продавца», то есть под действием обмана, согласилась и посредством установленного в ее мобильном телефоне мобильного приложения «СберБанк Онлайн», осуществила перевод принадлежащих ей денежных средств в размере 6 500 рублей с банковского счета №, открытого на ее имя и обслуживаемого в отделении ПАО «СберБанк России», указав при переводе номер электронного кошелька АО «КИВИ Банк» №, к которому подключён абонентский номер телефона +№, находящийся в пользовании ФИО6. Тем самым ФИО6 путем обмана совершил хищение денежных средств, принадлежащих ФИО2, в сумме 6 500 рублей[1].

Регистрация в социальной сети предполагает внесение персональных сведений о пользователе аккаунта, которому присваивается идентификатор (ID пользователя). Процесс регистрации связан с подтверждением данных о пользователе, для этого на указанный адрес электронной почты (номер мобильного телефона) отправляется запрос в виде ссылки (СМС-сообщение с кодом). Выявление данной информации позволит направить запрос организации-владельцу с целью получения данных о физическом лице, на которое зарегистрирован соответствующий аккаунт, о дате и времени регистрации, IP-адресе устройства, с которого осуществлялась регистрация или последний выход, электронной почте, абонентском номере, указанном при регистрации, и других сведений. Однако в настоящее время владельцами многих социальных сетей и сервисов для общения являются зарубежные компании, что затрудняет или делает невозможным процесс получения такой информации.

Осмотр страницы аккаунта в социальной сети предполагает отражение в протоколе следующих сведений:

– веб-браузер, через который осуществляется выход в Интернет, вид социальной сети и ее электронный адрес;

---

[1] Приговор № 1-209/2024 от 15 июля 2024 г. по делу № 1-209/2024 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

– логин и пароль пользователя, под которым осуществляется вход, его ФИО, «никнейм» (имя пользователя в сети);

– сведения об информационном содержании страницы: «статус» – визитная карточка владельца аккаунта, переписка, фотографии (представляющие криминалистический интерес), сведения о посещении.

Рассмотрим уголовное дело № 1-234/2021, возбужденное по факту совершения мошеннических действий, заключающихся в осуществлении телефонных звонков владельцам стационарных абонентских номеров и сообщении им заведомо ложных сведений о совершении их родственником дорожно-транспортных происшествий с целью побудить их к добровольной передаче денежных средств, чтобы помочь родственнику избежать уголовной ответственности за содеянное. В ходе предварительного расследования был обнаружен и изъят телефон «MEIZU», при осмотре которого установлено наличие программы «Telegram». При осмотре программы было установлено имя пользователя – Ю. А. С. (никнейм «Bla Bla»), от которого потерпевшая получала сообщения, и переписка с абонентом под ником «MONO» за период 5–7 мая 2021 года, содержащая информацию о совершенных Ю. А. С. преступлениях[1]. Осмотр телефона и содержания программы «Telegram» признаны допустимым доказательством.

Программа Telegram позволяет использовать для общения секретный чат, сохраняющий полную анонимность пользователей, и уничтожать сообщения по таймеру. Поэтому при осмотре переписки необходимо отключить автоудаление сообщений («пользователь» – «еще» – «автоудаление» – «выключить»).

В некоторых социальных сетях есть возможность делиться видео-, фотоизображениями, текстом и другими файлами, которые защищаются сквозным шифрованием и исчезают через 24 часа, при этом возможность просмотра существует при условии разрешения просмотра владельцем аккаунта. В случае их обнаружения следует просмотреть с возможностью записи.

В ходе осмотра аккаунтов в социальных сетях возможно осуществление снимков экрана устройства, которые подлежат осмотру. Логи-файлы, выдержки из внутренней и внешней аналитики и статистики по сайту подлежат распечатке[2] и приобщению к материалам уголовного дела.

Следует изучить историю просмотров веб-сайтов, кэш браузера (временные файлы), cookie-файлы, позволяющие осуществлять аутентифика-

---

[1] Приговор Ленинского районного суда г. Пензы (Пензенская область) от 20 сентября 2021 г. по делу № 1-234/2021 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

[2] Багмет А. М., Быков В. В., Скобелин С. Ю. Цифровые следы преступлений : монография. Москва : Проспект, 2023. С. 29.

цию пользователя. История просмотров сайтов хранится либо в настройках самого браузера, либо же вместе с временными файлами. Кэш браузера (временные файлы) сохраняется на локальном диске устройства. Cookie-файлы содержат информацию об адресе сайта, который создал этот файл, времени создания и сроке актуальности этого cookie. Все эти файлы, включая индивидуальные настройки пользователя, сохраняются на его компьютере. Эти данные позволяют в подробностях восстановить последовательность просмотра пользователем веб-сайтов.

Так, гр. Н-в М. А., преследуя цель незаконного обогащения, имея умысел на хищение чужого имущества в крупном размере путем обмана, создал интернет-магазин – Общество с ограниченной ответственностью (далее – Общество) под предлогом осуществления оптовой торговли электрическими, неэлектрическими бытовыми товарами и приборами. Не имея намерений и реальной возможности исполнять обязательства по закупу и доставке товаров, оплаченных физическими и юридическими лицами, гр. Н-в М. А. обманным путем похищал денежные средства граждан и был признан судом виновным в совершении мошенничества с причинением ущерба в крупном размере[1].

В указанном случае были установлены регистрационные данные на доменное имя, логи-файлы взаимодействия с доменных имен и сведения от платежей регистратору доменных имен, следы от взаимодействия с хостинг-провайдером, у которого размещен веб-сайт, реклама сформированного сайта, следы переписки с потерпевшими, сведения о приеме заказа.

Получить информацию о владельце домена возможно посредством сервиса https://www.whois.com, где в поле для запросов указывается название сайта, например crimtest (рис. 16).

На ресурсе CY-PR.com возможно установить хостинг-провайдера, на оборудовании которого размещена интернет-страница, информацию о регистрации, владельце (в случае если владелец верифицирован) (рис. 17).

Данная информация подлежит последовательной фиксации в протоколе осмотра. В последующем следователь может направить соответствующие запросы в адрес домен-регистратора, хостинг-провайдера.

Учитывая, что достаточно распространены веб-интерфейсы к электронной почте, при помощи восстановления просмотренных пользователем веб-страниц можно установить получение и отправку им сообщений электронной почты через такой веб-интерфейс[2]. В этой связи кримина-

---

[1] Приговор Ленинского городского суда г. Тюмени № 1-20/2019 1-718/2018 от 16 мая 2019 г. по делу № 1-20/2019 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

[2] Калмыков И. А., Пелешенко В. С. Компьютерная криминалистика : лабораторный практикум. Ставрополь : Северо-Кавказский федер. ун-т, 2017. 84 с. – URL: https://www.iprbookshop.ru/69392.html.

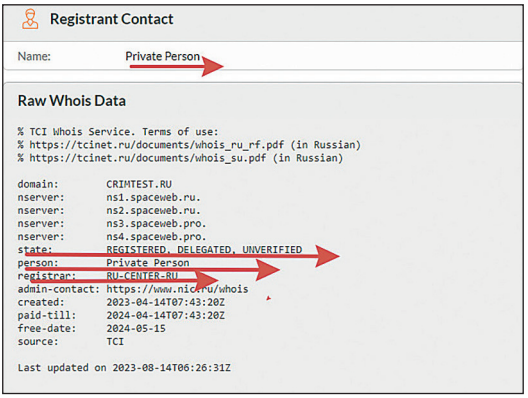


Рис. 16. Скриншот ответа с сервиса https://www.whois.com
с информацией о сайте crimtest.ru

Рис. 17. Скриншот ответа с сервиса https://www.cy-pr.com/a/crimtest.ru
с информацией о сайте crimtest.ru

листический интерес представляют и электронные письма, переданные посредством электронной почты. Быстрота, удобство, надежность и возможность постоянного доступа в любом месте делает сервис электронного почтового обмена привлекательным для постоянного использования, в том числе и при совершении преступления.

Лицу, участвующему в расследовании преступлений в сфере ИТТ, необходимо знать про формат EML – это стандартный файловый формат, используемый для представления почтовых сообщений, включая все их составляющие (текст, вложения, метаданные и др.).

Структура электронного письма следующая:

1. Заголовок SMTP-протокола (от англ. Simple Mail Transfer Protocol – «протокол передачи почты»), полученного сервером. В большинстве

случаев эта информация недоступна конечному получателю, который использует не-SMTP-протоколы (POP3, IMAP) для доступа к почтовому ящику. Для возможности контроля работоспособности системы эта информация обычно сохраняется в журналах почтовых серверов некоторое время.

2. Само письмо (в терминологии протокола SMTP – «DATA»):

а) заголовок письма, иногда называемый по аналогии с бумажной почтой конвертом (англ. «envelope»). В заголовке указывается служебная информация и пометки почтовых серверов, через которые прошло письмо, пометки о приоритете, адреса и имена отправителя и получателя письма, тема письма и другая информация;

б) «тело» письма, в котором находится собственно текст письма. Согласно стандарту, в «теле» письма могут находиться только символы ASCII.

В структуре заголовка письма имеются сведения об имени и адресе электронной почты отправителя, имени и электронном адресе получателя, которые заполняются обязательно. Тема – необязательное, но желательное для заполнения поле, а также адреса других абонентов, получающих копии сообщения. Date – дата отправления сообщения; Reply-to – электронные адреса, на которые отправляется ответ (они могут отличаться от адреса отправителя); Recived – различные интернет-серверы, пересылавшие сообщение от отправителя к получателю; Content-type – формат составления передаваемого сообщения и возможные приложения к нему; Content-Transfer-Encoding – способ передачи данных (7–8-битовое сообщение и др.); Message-ID – номер идентификации сообщения; X-mailer – программа передачи сообщений по электронной почте[1].

Рассмотрим на примере почтовой службы «Mail.ru» способ получения письма в формате EML для последующего его анализа:

1. Необходимо открыть интересующее письмо и в меню управления этим письмом нажать ●●● – перейти во вкладку «Еще» и выбрать «Скачать на компьютер».

2. Письмо сохранится в загрузках в формате EML (рис. 18).

Файлы EML могут быть использованы для анализа почтовой корреспонденции, включая извлечение метаданных, содержимого письма и вложений.

Таким образом, из файла EML установлено, что устройству, с которого было отправлено письмо, назначен IP-адрес 178.154.239.208, указывающий на сервер forward500c.mail.yandex.net.

---

[1] Третьякова Е. И., Босхолов С. С., Щербина Р. П. Возможности деанонимизации лиц, совершающих мошенничество с применением спуффинг-атак // Криминалистика: вчера, сегодня, завтра. 2021. № 4 (20). С. 111.

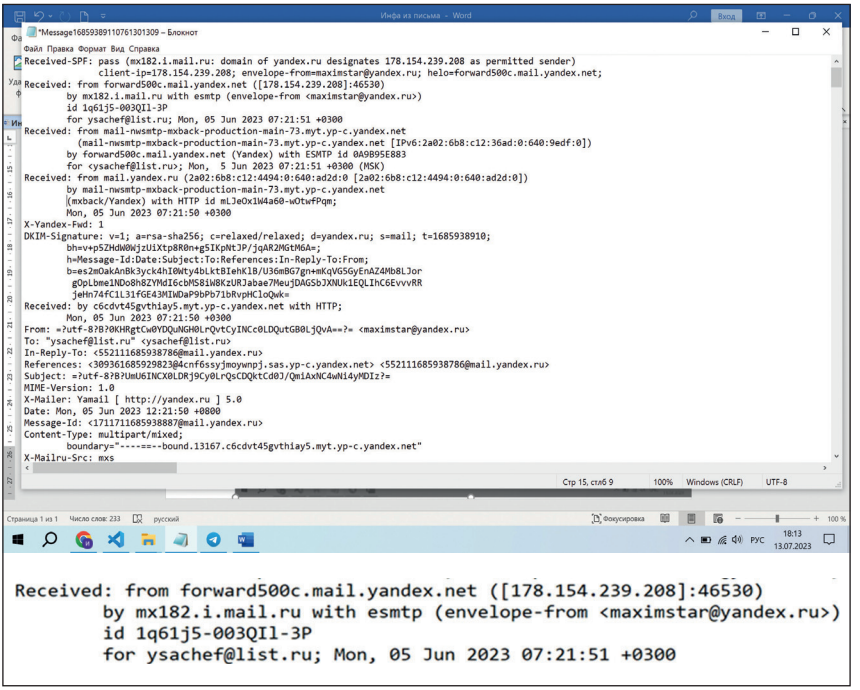


Рис. 18. Скриншот файла EML

Однако нередко преступники при совершении преступления применяют E-mail-spoofing[1], изменяя информацию об отправителе, показанную в электронной почте (поле «От»), используя сервис VPN или Прокси-сервер, которые способствуют анонимной работе в сети Интернет.

Реализуя требование ч. 6 ст. 166 УПК РФ, следователь после проведенного осмотра обязан ознакомить участников следственного действия с его результатами, занесенными в протокол, что должно быть подтверждено подписями.

Соблюдение указанных рекомендаций по осмотру компьютерных устройств позволит выявить криминалистически значимую информацию о способе, характере преступной деятельности, месте и времени совершения преступления. Грамотная работа по ее изъятию и содержательная фиксация позволят сформировать достаточный объем достоверных доказательств, что будет способствовать созданию условий, направленных на противодействие преступным проявлениям в рассматриваемой сфере.

[1] Технический прием изменения подлинности информации об отправителе.

Контрольные вопросы

1. Что относится к компьютерным устройствам и какие криминалистические рекомендации следует соблюдать при их осмотре?
2. Какую криминалистически значимую информацию можно получить при просмотре истории браузера?
3. Где хранятся кэшированные данные посещенных страниц (картинки, скрипты и прочее)?
4. Какие требования предъявляются к упаковке электронных носителей информации?
5. Предъявляются ли какие-либо требования к хранению электронных носителей информации, признанных вещественными доказательствами?
6. Назовите структуру электронного письма.

§ 3. Тактика допроса

Допрос как средство получения доказательств является самым распространенным следственным действием, которое проводится по каждому расследуемому уголовному делу. Такая популярность допроса обусловлена, с одной стороны, его высочайшими информационными возможностями, а с другой – простотой проведения, надежностью и быстротой получения результата[1].

Показания участников уголовного судопроизводства (подозреваемого, обвиняемого, потерпевшего, свидетеля, специалиста и эксперта) используются в качестве доказательств по уголовному делу, получать которые следует в четком соответствии с нормами уголовно-процессуального законодательства, поскольку их нарушение влечет за собой признание доказательств недопустимыми.

УПК РФ к недопустимым доказательствам относит показания подозреваемого, обвиняемого, данные в ходе досудебного производства по уголовному делу в отсутствие защитника, включая случаи отказа от защитника, и не подтвержденные подозреваемым, обвиняемым в суде; показания потерпевшего, свидетеля, основанные на догадке, предположении, слухе; а также показания свидетеля, который не может указать источник своей осведомленности (ст. 75).

Допрос представляет собой судебное и следственное действие, состоящее из получения и фиксации в определенной уголовно-процессу-

---

[1] Третьякова Е. И. Допрос несовершеннолетнего: процессуальные и тактические аспекты // Деятельность правоохранительных органов в современных условиях : сб. мат-лов XXIV междунар. науч.-практ. конф., Иркутск, 6–7 июня 2019 г. / Восточно-Сибирский институт МВД России. Иркутск : Восточно-Сибирский институт МВД России, 2019. С. 250–252.

альным законом форме показаний обвиняемого, подозреваемого, подсудимого, потерпевшего, свидетеля или эксперта об обстоятельствах, известных им, и других данных, которые имеют значение для правильного разрешения уголовного дела[1].

Основная задача допроса сводится к получению показаний, входящих в предмет доказывания по уголовному делу.

Общие положения тактики допроса сводятся к соблюдению законности, объективности и полноты получения показаний с учетом личности допрашиваемого лица, а также активности и целеустремленности следователя при проведении допроса. Следователь должен быть заинтересован в получении достоверной информации, известной допрашиваемому лицу, в полном объеме, применяя в случае необходимости тактические приемы, а ее оценка должна быть объективной.

Познавательные возможности допроса достаточно велики, т. к. рассматриваемое следственное действие может быть проведено для выяснения любых обстоятельств, которые входят в предмет доказывания. Однако, несмотря на внешнюю простоту допроса как следственного действия, не следует забывать о сложности установления психологического контакта с допрашиваемым; об адекватном восприятии устной речи; о правильном отражении в протоколе показаний, о преодолении добросовестного заблуждения или лжи[2].

В криминалистической тактике рекомендации по применению тактических приемов зависят от видов проводимых допросов.

При расследовании преступлений, совершенных с использованием ИТТ, проводятся следующие виды допросов: допрос протерпевшего, свидетеля, подозреваемого, обвиняемого, эксперта, специалиста. Допрос может проходить в конфликтной или бесконфликтной ситуациях, с участием третьих лиц и без таковых. В качестве такого дополнительного участника в нашем случае выступает специалист.

Как и любое следственное действие, допрос состоит из подготовительного, рабочего и заключительного этапов.

Успех проведения допроса во многом зависит от качественной подготовки к его проведению, в ходе которой следователь решает криминалистические, специальные и психологические задачи, реализовать которые необходимо в ходе проведения следственного допроса. Суть криминалистической подготовки сводится к изучению материалов уголовного дела, личности допрашиваемого лица; к выбору места и времени проведения следственного действия, способа вызова на допрос; к определению круга участников, а также необходимых технических средств.

---

[1] Топорков А. А. Криминалистика : учебник. М. : Контракт, 2012. С. 274.

[2] Третьякова Е. И. Допрос несовершеннолетнего: процессуальные и тактические аспекты. С. 250.

Особого внимания требует специальная подготовка, особенно при допросе подозреваемого в совершении преступления с использованием ИТТ. Способ рассматриваемых преступлений имеет определенную специфику, и осведомленность следователя о функционировании ИТ-технологий позволит качественно провести следственное действие. Допрашиваемое лицо может использовать соответствующую терминологию, толкование которой должно быть осуществлено самим допрашиваемым, тем не менее следователь должен понимать, о чем идет речь, и для этого ознакомиться со специальной литературой, осуществить консультации со специалистом и при необходимости привлечь его к следственному действию. Кроме того, специальная подготовка позволит определить конкретный перечень обстоятельств, входящих в предмет допроса участника уголовного судопроизводства.

Психологическая подготовка к допросу сводится к оценке личности допрашиваемого лица и возможности применения тактических приемов при его допросе. Уголовно-процессуальное законодательство наделяет следователя процессуальной самостоятельностью в выборе тактики допроса.

В современных исследованиях, посвященных рассматриваемой теме, отмечено, что основные трудности, с которыми следователям приходится сталкиваться в ходе допроса при расследовании преступлений, совершенных с использованием ИТТ, связаны с терминологией, выбором тактических приемов воздействия, установлением контакта[1]. Тактические приемы, применяемые в ходе допроса, достаточно разработаны в теории криминалистики и применяются прежде всего для получения полных объективных показаний от допрашиваемого лица. Выбор тактики допроса в первую очередь зависит от информированности следователя о преступном событии, процессуального положения допрашиваемого лица, возможности и желания дать показания.

В теории криминалистической тактики выделяют бесконфликтные (благоприятные) и конфликтные (неблагоприятные) ситуации, складывающиеся при допросе.

Конфликтная ситуация характеризуется получением от подозреваемого частично или полностью ложных показаний, а также отсутствием у допрашиваемого желания давать показания.

В зависимости от остроты конфликта ситуации бывают:

1) со строгим соперничеством, когда допрашиваемый:

– дает полностью ложные показания;

– отказывается от дачи показаний;

2) без строгого соперничества, когда допрашиваемый:

---

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений : дис. … канд. юрид. наук. Москва, 2016. С. 78–79.

– дает показания только по одному эпизоду преступной деятельности;

– скрывает соучастников и подстрекателей;

– дает ложные показания относительно отдельных обстоятельств преступления[1].

Данная позиция допрашиваемого лица расценивается как противодействие расследованию, что определяет для следователя необходимость применения мер по его преодолению, прежде всего посредством применения тактических приемов.

Бесконфликтная ситуация характеризуется установленным психологическим контактом, способствующим конструктивному общению между следователем и допрашиваемым лицом. Конфликтная же ситуация имеет характер острого соперничества.

Приступая к допросу, следователь должен решить тактическую задачу по установлению психологического контакта, что и определяет в конечном итоге ситуацию допроса. При этом необходимо учитывать, что как для установления психологического контакта, так и для более-менее успешной реализации любых тактических приемов необходимо понимание оппонента, его интересов и ценностей, типичных способов реагирования на раздражители (например, что он будет делать в случае возникновения угрозы: нападать, убегать или впадет в ступор). В этой связи одним из важных элементов в структуре личности следователя являются его коммуникативные качества, которые требуют понимания людей, их интересов, особенностей их жизненной и правовой социализации, оценки положительных и отрицательных, сильных и слабых сторон личности, способности прогнозировать поведение участников уголовного процесса.

Одним из первых участников уголовного судопроизводства допрашивается потерпевший, признание лица в качестве которого осуществляется незамедлительно после принятия решения о возбуждении уголовного дела или после получения данных о нем. Однако по некоторым преступлениям, например связанным с незаконным оборотом наркотических средств, совершенным с использованием ИТТ, потерпевший как участник уголовного судопроизводства де-юре отсутствует.

Допрос потерпевшего осуществляется в соответствии с требованиями ст. ст. 187–191 УПК РФ на досудебной стадии и ст. 277 УПК РФ – в рамках судебного следствия.

При допросе потерпевшему разъясняются права:

– давать показания на родном языке или языке, которым он владеет;

– отказаться свидетельствовать против самого себя, своего супруга (супруги) и других близких родственников (ст. 51 Конституции Российской Федерации).

---

[1] Цветков Н. А. Тактика допроса подозреваемого и обвиняемого в конфликтной ситуации // Вестник современных исследований. 2018. № 11 (26). С. 334.

При этом он должен быть предупрежден об уголовной ответственности за дачу заведомо ложных показаний (ст. 307 УК РФ), за отказ от дачи показаний (ст. 308 УК РФ), и о том, что его показания будут использованы в качестве доказательств по уголовному делу, в том числе в случае его последующего отказа от них.

Процессуальные же требования сводятся к соблюдению временных ограничений допроса. Общая продолжительность допроса без перерыва не должна превышать 4-х часов, при этом в течение дня допрос не может длиться более 8-ми часов.

Традиционно потерпевший заинтересован в предоставлении следователю полной и объективной информации о преступлении, которой он располагает. Однако потерпевший может стесняться своей некомпетентности в правовой, финансовой или технической сферах и недоговаривать о некоторых известных ему обстоятельствах. Кроме того, отсутствие у него знаний о функционировании информационных технологий и их возможностях может исказить показания. Поэтому при его допросе чаще всего складываются благоприятные или конфликтные ситуации без строгого соперничества. Следователь, приступая к допросу потерпевшего и устанавливая психологический контакт, должен проявлять тактичность, доброжелательность и вежливость.

Тактика допроса в таких ситуациях сводится к применению приемов активизации памяти допрашиваемого лица, ассоциативных связей, детализации показаний с целью выяснения полноценной информации, которая даже косвенно свидетельствовала бы о способе совершения преступления, применяемом преступником, постановки уточняющих и контрольных вопросов, которые должны быть краткими, ясными, не таить в себе двусмысленности и содержание которых должно исключать информацию, наводящую на тот или иной ответ. В качестве основного тактического приема активизации памяти потерпевшего следует выделить демонстрацию действий, которые выполнялись им на компьютерном устройстве. При этом следователь должен контролировать ситуацию с целью исключения появления тактического риска. Кроме того, рекомендуется к допросу привлекать необходимого специалиста.

В криминалистической тактике допроса при расследовании преступлений, совершенных с использованием ИТ-технологий, интерес представляют и обстоятельства, выясняемые при его проведении. Предмет допроса определяется с учетом конкретного вида преступления, совершенного с использованием ИТТ. Обязательному выяснению подлежат обстоятельства, подлежащие доказыванию (ст. 73 УПК РФ).

Криминалистическая тактика рекомендует соблюдать логичность и последовательность в выяснении сведений. В этом случае следует разделить обстоятельства, подлежащие выяснению, на группы: предшеству-

ющие совершению преступления, касающиеся самого преступного события, и следующие после совершения преступления.

Например, по уголовному делу № 1-284/2022 показания потерпевшего были следующего содержания:

«…Он работал в ателье «<данные изъяты>» по адресу: *адрес скрыт*, *адрес скрыт*. К нему на работу примерно в 10 часов пришел его знакомый ФИО2. Он его знает около 12 лет, находятся в дружеских отношениях. В долговых обязательствах друг перед другом не состоят. ФИО2 сидел у него в мастерской и пил чай, они общались с ним на общие темы. Через некоторое время ФИО2 попросил у него сотовый телефон, чтобы выйти в Интернет. Он разрешил ФИО2, разблокировал телефон и передал телефон ФИО2. Он видел, как ФИО2 находился в социальных сетях с его телефона, после чего ФИО2 допил чай и ушел. Что именно делал в социальных сетях, он не видел, так как он работал, каких-либо подозрений к ФИО2 не было, он ему доверял. Когда ФИО2 ушел, он решил произвести перевод денежных средств. Зашел в приложение «<данные изъяты>» и увидел уведомление, что с его банковского счета списались денежные средства в сумме <данные изъяты> рублей. Получатель «ФИО27 ФИО14». Данный перевод он не совершал, и получатель ему был неизвестен. Он понял, что деньги перевел ФИО2. Он начал звонить ФИО2, но он трубку на него не взял. Тогда он решил обратиться в полицию. В результате кражи ему причинен ущерб в сумме <данные изъяты>. Переводить денежные средства он ФИО2 не разрешал. При нем имеется выписка с ПАО «<данные изъяты>» о движении денежных средств с его банковской карты, в которой указан данный перевод на сумму <данные изъяты>, а также детализация <данные изъяты>» по его абонентскому номеру за *дата скрыта*. Кроме ФИО2, никто доступ к его телефону не имел, он считает, что ФИО2 совершил перевод через СМС-сообщения по номеру 900[1]».

Из этого следует, что к группе обстоятельств, предшествующих преступному событию против собственности «кража с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ), мошенничество, мошенничество с использованием электронных средств платежа», относятся сведения, характеризующие наличие предмета посягательства и его основные характеристики:

– наличие средства платежа, банкового счета;
– организация открытия счета, реквизиты и дата открытия;
– условия обслуживания и способы использования платежного средства;

[1] Приговор Шелеховского городского суда Иркутской области № 1-284/2022 от 14 декабря 2022 г. по делу № 1-284/2022 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

– привязано ли платежное средство к номеру мобильного устройства, если да – то к какому;

– оператор мобильной сети и наличие приложения банка на устройстве;

– источник пополнения платежного средства, сумма денежных средств, имеющихся на счете, последняя дата использования и назначение платежа;

– круг лиц, имеющих доступ, а также право и/или возможность использования платежного средства;

– кто мог незаконным способом получить сведения о платежном средстве (путем передачи потерпевшим платежного средства иным лицам, несоблюдения правил его использования).

К типичным сведениям, касающимся преступного события или возникшим в момент его совершения, относятся:

– обстоятельства, характеризующие способ совершения преступления: в чем конкретно выражались действия преступника, имели ли место обман или злоупотребление доверием. Сопровождались ли действия преступника СМС-рассылкой или рассылкой электронных писем, с какого номера или адреса электронной почты поступали, и их содержание. Детализация показаний потерпевшего относительно способа совершения преступления позволит подтвердить квалификацию преступного деяния;

– обстоятельства, характеризующие время совершения преступления: осуществлялась ли переписка с преступником и посредством чего, период ее осуществления и содержание; конкретное время совершения платежной операции и наличие документов, ее подтверждающих;

– к иным обстоятельствам совершения преступления могут быть отнесены: сведения об используемом компьютерном устройстве, способ осуществления связи с преступником, способ передачи предмета хищения, посредством чего и где осуществлялась операция;

– характер и размер причиненного ущерба: какова сумма похищенного имущества, доход семьи, наличие иждивенцев и кредитных обязательств; является ли ущерб значительным.

Обстоятельства, следующие после совершения преступления:

– когда и как потерпевший понял, что совершено преступление;

– какие действия предпринял;

– кому сообщил о происшествии.

Например, потерпевшая ФИО1 по обстоятельствам произошедшего показала, что является предпринимателем. Она как физическое лицо заказала бытовую технику на сайте ООО «<данные изъяты>: 2 телевизора, 10 шуруповертов, 6 соковыжималок, 10 блендеров на сумму 45 812 рублей 71 копейку, с комиссией вышло 46 200 рублей. При заказе товара ее в первую очередь привлекли цены, поскольку они были гораздо ниже, чем в <адрес>, откуда осуществляется доставка товара. Для

сравнения: у других продавцов в <адрес> аналогичный товар стоит 20 000 рублей, в <адрес> – 17 000 рублей, ООО <данные изъяты>» предлагало данный товар по цене 15 000 рублей. Кроме того, ее привлекло место нахождения магазина – в <адрес> и бесплатная доставка. Срок поставки должен был быть 1 месяц, однако сайт магазина перестал работать, товар она не получила. Она обратилась в <данные изъяты>, однако денежные средства ей не вернули, товар не поставили. Также она связывалась с руководителем ООО «<данные изъяты>» ФИО49, поскольку он был указан на сайте как директор ООО «<данные изъяты>», который ей пояснил, что интернет-магазин оказался мошенническим. Ей причинен ущерб, поскольку данный товар она заказала в целях исполнения и поставки по государственному контракту. Ущерб является для нее значительным, поскольку на иждивении у нее 2 малолетних детей, общий доход семьи составляет около 70 000 рублей, доход нестабильный с учетом характера ее работы (предпринимательская деятельность), у нее имеются кредитные и ипотечные обязательства. Кроме того, показала, что, поскольку товар был заказан для поставки по государственному контракту, но не был ею поставлен, она потратила дополнительные средства для приобретения нового товара, к ней были предъявлены штрафные санкции за нарушение сроков поставки товара – около 50 000 рублей. Заявляет гражданский иск, полностью его поддерживает[1].

При допросе потерпевшего при мошенничестве, совершенном через Интернет, или мобильном мошенничестве следует выяснить:

– сведения об адресе интернет-сайта «магазина», номера телефонов, с которых/на которые звонили;

– осуществлялась ли переписка, с какого устройства, ее содержание, дословное содержание разговора, кем представился звонивший;

– какую информацию сообщил, что предлагал сделать, точная последовательность действий;

– какие действия выполнил потерпевший;

– описание голоса, манеры строить фразы; характерные особенности речи и голоса преступника, возможность его опознания, имеется ли запись разговора на мобильном телефоне;

– установить круг лиц, состоящих в близких, семейных либо рабочих отношениях, которым могло быть известно о наличии денежных средств на банковских счетах;

– кто имел возможность доступа к управлению счетами потерпевшего, в том числе к его мобильному телефону;

---

[1] Приговор Ленинского городского суда г. Тюмени № 1-20/2021-718/2018 от 16 мая 2019 г. по делу № 1-20/2019 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

– поступали ли ему в период, предшествующий хищению денежных средств, СМС-сообщения или электронные письма с указанием попыток осуществления транзакций, которые он не совершал;

– подавал ли объявления с указанием своих личных данных на сайтах в сети Интернет, и если да, то каких;

– сумма и подробный способ передачи/перевода денежных средств (блиц-переводом, нарочным, курьером, посредством банкомата, банковских приложений и иные);

– абонентский номер телефона, банковской карты, банковского счета, на которые переведены денежные средства;

– имеются ли у него документы, подтверждающие факт списания денежных средств, а также общения с неустановленным лицом, совершившим хищение денежных средств (в том числе скриншоты, переписка);

– не было ли сбоев в работе аккаунтов в социальных сетях;

– какова точная сумма причиненного преступлением ущерба. При решении вопроса о значительности причиненного вреда необходимо исходить из имущественного положения физического лица, выяснив размер его личных доходов, доходов семьи, наличие иждивенцев, кредитных или иных имущественных обязательств.

При допросе потерпевшего (мошенничество и преступления в сфере компьютерной информации) следует выяснить:

– содержание компьютерной информации, кто является ее владельцем и кто имел к ней доступ и право на использование, на каких носителях она хранилась (запоминающие устройства электронно-вычислительных машин, внешние электронные носители) и в какой форме;

– посредством каких компьютерных устройств обрабатывалась и передавалась информация, идентификационные признаки этих устройств;

– какие действия в отношении компьютерной информации осуществлены: неправомерный доступ или ввод, удаление, блокирование, модификация или иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации в целях хищения чужого имущества или приобретения права на чужое имущество. Полученные сведения позволят подтвердить наличие признаков мошенничества в сфере компьютерной информации или неправомерного доступа к ней;

– какие последствия наступили: уничтожение, блокирование, модификация либо копирование компьютерной информации; какой материальный ущерб причинен;

– защищено ли устройство от свободного доступа к его содержимому, и защищены ли сведения (сообщения, данные) методами криптографии и стеганографии;

– установлены ли на компьютерной технике программы защиты от несанкционированного доступа и антивирусные программы;

– подключено ли устройство, являющееся носителем информации, к проводной или беспроводной (Wi-Fi) сети Интернет;

– кто мог знать о наличии соответствующей компьютерной информации.

Приведенный перечень обстоятельств не является исчерпывающим, его расширение зависит от вида совершенного преступления, осведомленности потерпевшего о механизме преступной деятельности и информированности о функционировании информационно-телекоммуникационных технологий.

По преступлениям, совершенным с использованием ИТТ, определенную ценность представляет допрос специалиста или эксперта.

УПК РФ относит показания эксперта/специалиста к доказательствам по уголовному делу. При этом показания эксперта даются по существу разъяснения или уточнения данного им заключения, а специалист в ходе допроса разъясняет обстоятельства, требующие специальных знаний, или высказывает свое мнение. Эксперт может быть допрошен только после проведенной им экспертизы, а специалист – при возникновении такой необходимости.

При расследовании преступлений, совершенных с использованием информационных технологий, как правило, возникает необходимость разъяснения заключения компьютерной экспертизы, допрос эксперта по которому для следователя, зачастую не обладающего знаниями в рассматриваемой сфере, является весьма сложным.

Поскольку задачи судебно-компьютерной экспертизы многоаспектны, начиная с поиска на исследуемых объектах информации определенного содержания (текстовых файлов, информационных баз данных, графических и видеофайлов, содержащих какие-либо ключевые аспекты) и заканчивая восстановлением удаленной информации, в ходе допроса эксперта может быть выяснена и его некомпетентность по какому-либо вопросу. В этом случае следователь должен решить вопрос о назначении повторной экспертизы.

Определяя предмет допроса эксперта, следователь в первую очередь должен руководствоваться перечнем тех вопросов, которые он задавал эксперту при назначении экспертизы, и выводами по ним, требующими разъяснения.

Допрос эксперта проводится в случаях, если:

– выводы, сформированные экспертом, требуют общего разъяснения, почему и как они сформированы;

– в ходе исследования не представилось возможным решить поставленные перед экспертом вопросы;

– в заключении сформирован вывод, противоречащий иным имеющимся по уголовному делу доказательствам;

– сформирован отрицательный вывод;

– со стороны защиты поступило ходатайство о внесении дополнительных вопросов;

– в заключении эксперта и протоколах следственных действий имеются расхождения в описании представленных на экспертизу объектов и их упаковки;

– в заключении недостаточно разъяснена применяемая методика.

С тактической точки зрения допрос эксперта, проводившего компьютерную экспертизу, для следователя сложен в части понимания применяемой экспертом методики и формирования выводов. Эксперт, обладая знаниями в области компьютерных технологий и давая показания, может использовать специфичную терминологию, считая, что следователь компетентен в рассматриваемой сфере. В этом случае следователь должен максимально детализировать показания эксперта и просить разъяснять значения терминов. В целом же эксперт как иной участник уголовного судопроизводства заинтересован в разъяснении данного им заключения, и поэтому его допрос осуществляется в благоприятной ситуации.

В практике наблюдается негативная тенденция, когда следователь, не имея возможности всесторонне оценить полученное заключение ввиду отсутствия специальных знаний, отказывается от проведения допроса эксперта.

Допрос специалиста – более распространенное следственное действие, в том числе по преступлениям, совершенным с использованием ИТТ. Область его специальных знаний при допросе по рассматриваемым преступлениям, как правило, тоже ограничивается компьютерными технологиями. Так, нередко следователь осуществляет допрос специалиста с целью разъяснения способа совершения преступления, механизма образования цифровых следов, способа анонимизации лиц, совершивших такие преступления, и методов деанонимизации этих лиц. Кроме того, нередко возникает необходимость допроса специалиста по факту его участия в следственном действии и проводимых в ходе него конкретных мероприятиях, например по изъятию электронных носителей или дампа памяти при осмотре места происшествия, обыске или выемке.

В этом случае примерный перечень обстоятельств, требующих пояснения, может быть следующим:

– какие устройства были обнаружены, и были ли они снабжены средствами экстренного уничтожения информации;

– какие способы нейтрализации средств экстренного уничтожения информации были применены специалистом, и какой результат достигнут;

– были ли выявлены признаки применения «облачных» технологий хранения данных;

– какие средства шифрования, криптографии и стеганографии применялись, методы их преодоления и содержание;

– были ли обнаружены резервные хранилища, их содержание;

– осуществлялось ли изъятие устройства полностью, копировалась ли информация;

– какая существовала угроза удаления или уничтожения информации, на основании которой следователь отказал в удовлетворении поступившего ходатайства о ее копировании, и т. п.

Допросы эксперта и специалиста с тактической точки зрения не различаются. Для разъяснения вопросов, входящих в их компетенцию, рекомендуется применять тактические приемы детализации показаний для наглядности демонстрации действий на компьютерном устройстве или схематических зарисовок. При этом следователь должен держать ход допроса под постоянным контролем и анализировать полученную информацию с целью сопоставления ее с другими доказательствами, чтобы оперативно реагировать на возникшие противоречия путем постановки уточняющих и дополняющих вопросов.

Показания эксперта и специалиста протоколируются. Показания эксперта фиксируются в протоколе допроса эксперта. Что касается показаний специалиста, то имеется практика, когда они фиксируются в протоколе допроса свидетеля. Однако это недопустимо. Следует напомнить, что свидетелем является лицо, которому могут быть известны какие-либо обстоятельства, имеющие значение для расследования, и которое вызвано для дачи показаний. УПК РФ закрепляет перечень отдельных категорий лиц, не подлежащих допросу в качестве свидетеля, и в этом перечне нет специалиста. В этой связи допрос специалиста в качестве свидетеля делает необоснованным предъявление к нему требования профессиональной компетентности. Такая неправомерная подмена процессуальных статусов влечет изменение в совокупности процессуальных прав и обязанностей этих участников, определяющих границы возможного и необходимого их поведения в ходе уголовного судопроизводства.

Более того, в этом случае нарушаются нормы УПК РФ, поскольку специалист не может принимать участие в производстве по уголовному делу, если он является свидетелем по данному делу. Поэтому допрос специалиста в качестве свидетеля противоречит не только смыслу его уголовно-процессуального статуса, но и требованиям норм УПК РФ, а это значит, что его доказательственное значение может быть поставлено под сомнение.

Наиболее сложным для проведения при расследовании преступлений, совершенных с использованием ИТ-технологий, является допрос подозреваемого. Реализуя право подозреваемого на защиту, следователь должен обеспечить участие защитника по назначению или же выбранного подозреваемым защитника. Отказ от защитника должен быть письменно зафиксирован.

Готовясь к проведению допроса, следователь должен изучить материалы уголовного дела, а при необходимости – и специальную литературу,

изучить личность допрашиваемого лица, проконсультироваться со специалистом или же решить вопрос о его участии, убедившись в его компетентности.

Установление психологического контакта будет основополагающим фактором, определяющим выбор следователем тактики допроса. Поскольку в ходе допроса интересы следователя и допрашиваемого лица, как правило, не совпадают, допрос производится в условиях конфликтной ситуации, общение носит характер принудительности, что, соответственно, предопределяет сложность как в установлении контакта, так и в получении необходимой следователю криминалистически значимой и доказательственной информации.

Следователь должен быть готов к возможному осуществлению противодействия и применению тактических приемов его преодоления, направленных прежде всего на изобличение допрашиваемого во лжи.

Процесс изобличения допрашиваемого во лжи всецело основывается на применении тактических приемов эмоционального, логического воздействия и тактических комбинаций как совокупности таких приемов.

К приемам эмоционального воздействия относятся приемы воздействия на подозреваемого (на положительные качества личности) с целью склонить его к даче правдивых показаний, к признанию своей вины.

Возможность применения приемов логического воздействия зависит от информированности следователя о преступлении и наличия у него доказательств, опровергающих показания подозреваемого, которые возможно предъявить в ходе допроса. Детализация показаний, постановка контрольных и повторных вопросов, прием косвенного допроса и отвлечение внимания, прием прерывания допроса и создание легенды преувеличенной осведомленности следователя – все эти приемы используются в правоприменительной практике как методы преодоления противодействия при допросе.

Использование форсированного темпа допроса возможно в том случае, когда следователь достаточно компетентен в области информационных технологий, а для следователя, не имеющего должного уровня знаний в этой области, такой темп, наоборот, может послужить средством разоблачения созданной легенды о его осведомленности и компетентности. При допросе преступника, совершившего неправомерный доступ к компьютерной информации по мотивам демонстрации своих навыков, целесообразно имитировать ситуацию восхищения его действиями, что позволит установить психологический контакт с ним и мотивирует его рассказать о своих криминальных «достижениях»[1].

---

[1] Рудых А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : дис. … канд. юрид. наук. Ростов н/Д, 2020. С. 112.

Таким образом, тактические приемы, применяемые следователем в ходе допроса подозреваемого, направлены на преодоление возникшего конфликта и нежелания подозреваемого давать показания.

В начале допроса следователь должен определить уровень компетентности подозреваемого в области информационных технологий.

В этом случае следует выяснить:

– наличие, уровень и специальность или направленность образования;

– место работы, должность и перечень обязанностей;

– наличие навыков работы с конкретными компьютерными устройствами, программным обеспечением и уровень квалификации.

Об осведомленности и компетентности подозреваемого может свидетельствовать употребляемая им лексика. Так, подозреваемый может использовать специальные термины, компьютерный жаргон, иногда максимально снабжая ими свою речь с целью продемонстрировать свое превосходство над следователем, запутать его или ввести в заблуждение. В этой связи существенную помощь может оказать специалист, который способен сразу распознать ложь и тем самым нейтрализовать попытку противодействия расследованию. Кроме того, важно, чтобы именно подозреваемый, а не участвующий специалист, пояснил значения употребляемых им терминов, поскольку в различных отраслях компьютерных технологий одни и те же слова могут использовать в разных значениях, иногда отличных от общеупотребительных. Даже в словарях определения терминов могут существенно отличаться. Кроме того, некоторые начинающие «хакеры», желая показать свои «знания» в сфере информационных технологий, используют термины неправильно, не понимая их смысл.

Непосредственно предмет допроса, касающийся обстоятельств совершенного преступления, зависит от вида совершенного преступления.

Примерный перечень обстоятельств, подлежащих выяснению, может быть следующим:

1. Обстоятельства, касающиеся события преступления (объективные признаки преступления).

Например, по уголовному делу № 1-243/2020 Данилова Е. С. пояснила, что является специалистом офиса обслуживания и продаж ПАО «Вымпелком» в г. Октябрьский, расположенном по адресу: РБ, г. Октябрьский, 34 мкр., 8а, имеет навыки работы в компьютерной программе «1С», ознакомилась с нормативными документами и требованиями по информационной безопасности, имеет присвоенный индивидуальный и конфиденциальный логин и пароль, необходимые для работы в указанной компьютерной программе, содержащей персональные данные клиентов ПАО «Вымпелком» и персональные данные их лицевых счетов, которые охраняются Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите

информации»[1]. Умышленно, из корыстной заинтересованности, используя свое служебное положение, с целью неправомерного доступа к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ПАО «Вымпелком» и персональные данные их лицевых счетов, с целью ее модификации под своими индивидуальными и учетными данными осуществила доступ в компьютерную программу «1С», используемую сотрудниками ПАО «Вымпелком» для сервисного обслуживания абонентов оператора сотовой связи «Билайн». Не имея соответствующего заявления клиента, 17 января 2020 года в 16 часов 45 минут в офисе обслуживания и продаж ПАО «Вымпелком» выбрала абонентский номер №, зарегистрированный на Фур Ю. В., с привязанным к нему лицевым счетом, подделав заявление клиента на замену СИМ-карты, произвела перевыпуск СИМ-карты и модификацию компьютерной информации, получив возможность пользоваться лицевым счетом с находящимися на нем деньгами, принадлежащими ПАО «Вымпелком». 18 января 2020 года в 16 часов 45 минут в сети Интернет оплатила покупку товара на сумму 1 288,16 рублей, 18 января 2020 года в 16 часов 47 минут перевела на счет своей банковской карты №… деньги в сумме 14 850 рублей, 18 января 2020 года в 18 часов 49 минут в сети Интернет оплатила покупку товара на сумму 314,62 рублей, 19 января 2020 года в 8 часов 47 минут перевела на счет своей банковской карты № деньги в сумме 14 850 рублей, 19 января 2020 года в 8 часов 50 минут в сети Интернет оплатила покупку товара на сумму 1 112,05 рублей, тем самым совершив хищение денег, принадлежащих ПАО «Вымпелком», на сумму 32 414,83 рублей[2].

Таким образом, для преступлений в сфере компьютерной информации перечень обстоятельств, подлежащих выяснению, может быть следующим:

– как осуществлялась подготовка к совершению преступления;

– имели ли место неправомерный доступ к компьютерной информации или другие действия, и в чем конкретно они выражались;

– какое конкретно компьютерное устройство использовалось, его идентификационные признаки (модель, серийный номер), место его нахождения;

– какие виды операций совершались с компьютерной информацией, с какой целью и как;

---

[1] Об информации, информационных технологиях и о защите информации : Федер. закон № 149-ФЗ : принят Гос. Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. : послед. ред. // Официальный интернет-портал правовой информации : сайт. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264.

[2] Приговор Октябрьского городского суда Республики Башкортостан № 1-243/2020 от 29 июля 2020 г. по делу № 1-243/2020 // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

– к каким сетям компьютерное устройство подключено, какое имеется дополнительное оборудование, какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети);

– используются ли средства шифрования, криптографии и стеганографии в этом устройстве, и если да, то каким образом;

– в какую компьютерную систему (сеть) подозреваемому удалось проникнуть, и каким образом;

– какие меры защиты информации использовались, и как он их преодолел, какие программно-аппаратные комплексы использовались;

– каким образом была преодолена физическая, техническая и программная защита компьютерной информации;

– откуда подозреваемый мог узнать о наличии компьютерной информации, ее содержании, паролях (кодах) доступа к ней;

– к какой информации получил доступ, ее содержание;

– имеет ли подозреваемый в силу своего служебного положения право доступа к данной информации;

– время или период совершения преступных действий;

– другие данные о преступном событии.

Для иных преступлений, совершенных с использованием ИТТ:

– имело ли место хищение имущества: тайное, путем обмана или злоупотребления доверием, или же совершено иное преступление (сбыт наркотических средств), в чем конкретно выражались действия, как использовались информационные технологии в механизме преступной деятельности;

– наличие в пользовании телефона, его модель, номер абонента, на которого зарегистрирован, IMEI-номер;

– какое компьютерное устройство использовалось, его характеристики и место нахождения, к какой связи подключено, и ее поставщик;

– какие мессенджеры использовались для общения в процессе совершения преступления, с какого устройства, на кого зарегистрирован аккаунт;

– использовались ли средства анонимизации, и если да, то какие;

– как происходил выбор потерпевших, осуществлялся ли с ними предварительный контакт, какой и посредством чего, какая легенда использовалась;

– наличие банковских счетов, электронных кошельков, банковских карт, иных электронных средств платежа в пользовании, источник их пополнения;

– на какие счета переводились денежные средства и в каком объеме, на кого, когда и где они зарегистрированы;

– время или период совершения преступных действий;

– каким образом подозреваемый распорядился имуществом, полученным преступным путем;

– другие данные о преступном событии.

2. Обстоятельства, характеризующие субъективные признаки преступления:

– имел ли подозреваемый умысел на совершение преступления, когда и почему он сформировался;

– мотивы и цели совершения преступления;

– имелись ли соучастники, их персональные данные и действия каждого из них при совершении преступления;

– сведения о пользователе компьютерного устройства, аккаунте, который использовался при совершении преступления, на кого зарегистрирован, его характеристики.

3. Обстоятельства, характеризующие причиненный ущерб:

– какие последствия наступили: уничтожение, блокирование, модификация либо копирование компьютерной информации;

– причинен ли материальный ущерб, его размер;

– наступили ли тяжкие последствия, или создана ли угроза их наступления.

К тяжким последствиям постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 относит длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т. п.

Таким образом, при допросе подозреваемого следует выяснить все обстоятельства подготовки и совершения преступления, алгоритм использования информационных технологий в преступной деятельности.

Допрос обвиняемого проводится немедленно после предъявления ему обвинения. Следователь выносит постановление о привлечении лица в качестве обвиняемого при наличии достаточных доказательств, дающих основания для его обвинения в совершении преступления. Если обвиняемый отказался от дачи показаний на первом допросе, его повторный допрос по тому же обвинению может быть проведен только по просьбе самого обвиняемого. При допросе обвиняемого в случае его несогласия с предъявленным обвинением следователь в полной мере может применить тактический прием предъявления доказательств, поскольку их у него в распоряжении достаточное количество. Если обвиняемый согласен с предъявленным обвинением и желает давать показания, в случае необходимости следователь может применять тактические приемы, направленные на активизацию памяти допрашиваемого лица. В целом же с точки зрения тактики и предмета допроса допрос обвиняемого не отличается от допроса подозреваемого и проводится в соблюдением ранее рассмотренных рекомендаций.

Показания подозреваемого/обвиняемого заносятся в протокол допроса соответствующего участника уголовного судопроизводства, который составляется с соблюдением требований ст. ст. 166, 167, 190 УПК РФ. В протокол показания заносятся от первого лица и по возможности дословно. Соблюдение требования дословного протоколирования показаний при допросах подозреваемых/обвиняемых в ходе расследования преступлений, совершенных с использованием ИТТ, очень важно, особенно если допрашиваемые предоставляют информацию о механизме совершенного преступления.

С целью обеспечения этого требования следователь имеет возможность осуществить видеозапись следственного действия, о чем делается отметка в протоколе. Видеозапись подлежит просмотру участниками следственного действия, сохранению на съемном накопителе, который упаковывается, опечатывается и хранится при материалах уголовного дела.

В качестве средства устранения противоречий в показаниях ранее допрошенных лиц выступает очная ставка. Следует отметить, что очная ставка признается разновидностью допроса, однако является самостоятельным следственным действием. Кроме того, в теории криминалистического учения о противодействии расследованию преступлений очная ставка признается важным средством преодоления противодействия со стороны участников уголовного судопроизводства. Однако при расследовании преступлений, совершенных с использованием информационных технологий, следователи очень редко прибегают к ее возможностям, поскольку противоречия в показаниях допрашиваемых участников возникают, как правило, в связи с разной степенью их осведомленности или субъективностью восприятия ими фактов, а очной ставкой устранить такие противоречия невозможно.

В правоприменительной деятельности очная ставка при расследовании преступлений, совершенных с использованием ИТТ, проводится при возникновении существенных противоречий в показаниях двух подозреваемых лиц или подозреваемого и третьего лица, имеющего статус свидетеля по уголовному делу. В ходе очной ставки выясняется факт знакомства допрашиваемых лиц и их взаимоотношения. При этом следователь должен внимательно следить за реакциями, эмоциями, поведением участников очной ставки, контролировать ее ход и исключить ситуации возникновения тактического риска, связанные с изменением показаний участником, ранее давшим правдивые показания. В целом же тактические приемы психологического и логического воздействия, применяемые в ходе проведения очной ставки, идентичны тактическим приемам допроса.

Таким образом, допрос участников уголовного судопроизводства является распространенным и важным следственным действием, результат

которого признается доказательством по уголовному делу. Эффективность допроса зависит в том числе от соблюдения вышеобозначенных криминалистических рекомендаций по его проведению (качественная подготовка, установление психологического контакта, применяемые тактические приемы, полнота предмета допроса), а его доказательственное значение определяется соблюдением процессуальных требований.

Контрольные вопросы

1. Условия, влияющие на возникновение конфликтной и бесконфликтной ситуаций допроса.
2. Основные тактические приемы допроса в условиях конфликтной и бесконфликтной ситуаций.
3. Что влияет на определение предмета допроса участника уголовного судопроизводства?
4. Определите предмет допроса подозреваемого, совершившего мошенничество с использованием мобильного телефона.
5. Допрос эксперта и специалиста: основания проведения и предмет допроса.

§ 4. Тактика следственных действий, направленных на изъятие электронных носителей информации и компьютерной информации

К следственным действиям, направленным на изъятие электронных носителей компьютерной информации, в первую очередь следует отнести обыск и выемку. Изъятие электронных носителей информации и компьютерной информации с последующим приобщением их к материалам уголовного дела в качестве доказательств также осуществляется в ходе осмотра места происшествия, предметов и документов[1].

Обыск и выемка по делам о преступлениях, совершенных с использованием ИТТ, в большинстве случаев нуждаются в безотлагательном проведении, поскольку существует риск уничтожения (сокрытия, модификации) цифровых следов и их носителей со стороны заинтересованных лиц. Вместе с тем указанные следственные действия требуют организационно-технической подготовки.

Места проведения обыска в зависимости от отношения к нему подозреваемого можно условно разделить на три группы:

---

[1] Более подробно о тактике производства осмотра см. § 2 настоящей главы («Тактика осмотра»).

– место жительства подозреваемого и иных связанных с ним лиц (родственников, знакомых), а также иные принадлежащие им объекты (дачи, гаражи, автотранспорт и т. п.);

– место, где подозреваемый осуществляет трудовую и иную деятельность, а также арендуемые им объекты недвижимости (поскольку собственники (владельцы) обыскиваемых объектов непричастны к совершенному преступлению, они, как правило, не оказывают противодействия проводимым следственным и иным мероприятиям);

– территории организаций и предприятий, администрация которых осуществляет преступную деятельность, в т. ч. не связанную с расследуемым уголовным делом. В этом случае возможно оказание противодействия, вплоть до силового.

На подготовительном этапе обыска следователю необходимо осуществить следующие мероприятия:

– выяснить, какое информационно-телекоммуникационное оборудование находится в помещении, намеченном для проведения обыска, и по возможности установить его технические характеристики;

– установить, какие средства защиты информации и ИТ-техники от несанкционированного доступа находятся по месту обыска; по возможности выяснить ключи доступа и технические характеристики средств защиты;

– определить режим и технические системы охраны объекта, ИТ-техники и категорию обрабатываемой информации (общедоступная или конфиденциальная);

– выяснить, какие средства ИТ-техники используются, установить их тип, тактико-технические характеристики, категорию (общедоступные или конфиденциальные), абонентские номера, ключи (коды) доступа, позывные и т. п.;

– установить тип источников электропитания ИТ-оборудования (электросеть, автономные, бесперебойные, комбинированные) и расположение пунктов обесточивания помещения и аппаратуры, подлежащих обыску;

– пригласить соответствующих специалистов для подготовки и участия в следственном действии;

– подготовить соответствующие СКТ, специальную аппаратуру и материалы для поиска, просмотра, распаковки, расшифровки, изъятия и последующего хранения компьютерной информации, ИТ-техники и специальных технических устройств;

– определить дату, время и границы проведения обыска, время поиска и меры, обеспечивающие его конфиденциальность (важно, чтобы пользователь, владелец или оператор ИТ-техники не подозревали о предстоящем следственном действии и не работали в момент проведения обыска на ИТ-оборудовании);

– проинструктировать оперативных сотрудников и специалиста, осуществляющего фото- и видеофиксацию, о специфике проводимого следственного действия;

– по возможности изучить личность обыскиваемого пользователя (владельца) ИТ-техники, вид его деятельности, профессиональные навыки по владению ИТТ;

– при необходимости (большая обыскиваемая территория, возможное оказание обыскиваемыми сопротивления и т. п.) привлечь дополнительные силы (сотрудников оперативных подразделений, специального отряда быстрого реагирования);

– пригласить понятых, желательно обладающих базовыми знаниями в области ИТТ (на уровне не ниже пользователя соответствующих средств компьютерной техники, ИТ-оборудования, программного обеспечения), достаточными для понимания содержания производимого следственного действия. В качестве таких лиц могут выступать студенты, получающие технические специальности в образовательных организациях высшего образования либо информационно-технические специальности в образовательных организациях среднего профессионального образования, продавцы-консультанты салонов сотовой связи и компьютерных магазинов, специалисты по обслуживанию и ремонту компьютерной техники и т. п.

По прибытии к месту проведения обыска необходимо вести себя следующим образом:

– быстро и внезапно пройти на обыскиваемый объект (или одновременно в несколько помещений);

– при оказании сопротивления со стороны лиц, находящихся на объекте обыска (обыскиваемого, его родственников, охранников, сторожей, сотрудников организации и т. п.), принять срочные меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение;

– организовать охрану места обыска и наблюдение за ним. Охране подлежат: периметр обыскиваемых площадей; ИТ-техника; ЭНИ; все пункты (пульты) связи, охраны и электропитания, находящиеся на объекте обыска (в здании, помещении, на производственной площади); специальные средства защиты от несанкционированного доступа; хранилища ключей аварийного и регламентного доступа к ИТ-технике, помещениям и другим объектам (пульты, пункты, стенды, сейфы и т. п.).

Стоит обратить особое внимание на то, что перед началом производства любых следственных действий, непосредственно связанных с ИТ-техникой, средствами и системами их защиты, необходимо в обязательном порядке получать и анализировать с участием специалистов информацию о технологических особенностях функционирования вышеприведенных технических устройств, уровне их соподчиненности

и используемых средствах связи и телекоммуникации во избежание их разрушения, нарушения заданного технологического ритма и режима функционирования, причинения крупного материального ущерба пользователям и собственникам, уничтожения доказательств. В целях обнаружения скрытых или замаскированных ЭНИ, имеющих электронные компоненты, возможно применение средств их поиска, например нелинейных локаторов.

Следователю необходимо знать, что к изменению или уничтожению компьютерной информации, ее электронных носителей и ИТ-техники, которые впоследствии могут выступать в качестве доказательств по делу, приводят не только манипуляции с самой ИТ-техникой, но и включение или выключение ее электропитания, а также разрыв соединения между ее компонентами. Поэтому все электротехническое оборудование и средства электротехнических систем, имеющиеся на месте обыска, должны находиться до момента их осмотра специалистом в том пространственном положении и техническом состоянии, в котором они были в момент начала обыска. Для этого необходимо соблюдать следующие условия:

– запретить кому бы то ни было из находящихся на объекте обыска лиц (за исключением приглашенных специалистов) прикасаться к ИТ-технике и источникам питания электрооборудования с любой целью, даже в случае согласия обыскиваемого добровольно выдать искомый предмет, документ или информацию;

– запретить кому бы то ни было отключать-подключать электроснабжение объекта (указанные действия проводить только с согласия специалиста);

– в случае, если на момент начала обыска электроснабжение объекта отключено, до его восстановления следует отключить от электросети всё ИТ-оборудование, предварительно зафиксировав в протоколе схему его подключения к источникам электропитания, расположение, технические характеристики и порядок отсоединения от них ИТ-аппаратуры;

– не производить самостоятельно никаких манипуляций с электрооборудованием и ИТ-техникой, если результат заранее неизвестен;

– при настойчивых попытках обыскиваемого или других лиц, находящихся на месте обыска, получить доступ к ИТ-оборудованию, пунктам связи, управления и энергоснабжения, к другим техническим средствам, следует принять меры для удаления этих лиц в другое помещение (не подлежащее обыску) с одновременной фиксацией данного события в протоколе.

В случае наличия на объекте обыска беспроводного подключения к ИТ-сетям, а также в целях исключения возможности дистанционного воздействия на находящиеся информационно-технические средства и установления связи обыскиваемого с другими лицами целесообразно

использовать специальные технические средства подавления радиосигналов, имеющиеся у правоохранительных органов.

На обзорной стадии обыска необходимо:

1. Определить специальные средства защиты информации и ИТ-аппаратуру и отключить их от несанкционированного доступа, особенно те, которые автоматически уничтожают информацию и ЭНИ при нарушении процедуры доступа к ИТ-технике и компьютерной информации, порядка их использования и (или) установленных правил работы с ними; принять меры к установлению пароля, ключа санкционированного доступа и шифрования-дешифрования информации.

2. Установить наличие телекоммуникационной связи между средствами компьютерной техники, телекоммуникационным оборудованием и каналами электросвязи по схемам: «компьютер – компьютер»; «компьютер – управляющий компьютер»; «компьютер – периферийное устройство»; «компьютер – средство электросвязи»; «компьютер – канал электросвязи»; «периферийное устройство – периферийное устройство»; «периферийное устройство – канал электросвязи»; «канал электросвязи – периферийное устройство».

3. Определить ИТ-технику, находящуюся во включенном состоянии, и характер выполняемой ею операций и (или) программ. Особое внимание необходимо уделить терминальным печатающим и видеоотображающим устройствам (принтерам и мониторам). Распечатки информации (листинги) при необходимости должны быть изъяты и приобщены к протоколу следственного действия; изображение на экране монитора – изучено и детально описано в протоколе (можно также воспользоваться средствами фото- и видеофиксации либо сделать распечатку на бумаге с использованием специальных сканирующих программ).

4. При обследовании персонального компьютера (ноутбука, смартфона и т. п.) необходимо:

– установить активные программы, снять дамп памяти и скопировать информацию из открытых криптоконтейнеров (данные действия возможно производить только с участием квалифицированного специалиста!);

– произвести экспресс-анализ компьютерной информации, содержащейся на жестком (твердотельном) диске и в оперативной памяти компьютера, с целью получения криминалистически значимых сведений (интерес могут представлять файлы с текстовой и графической информацией).

5. Исключить возможность удаленного доступа к находящимся на объекте ИТ-средствам и оборудованию, включая мобильные телефоны (перевести их в авиарежим).

Детальная стадия обыска является очень трудоемкой и требует высокой квалификации как специалиста в области ИТТ, так и всей следственно-оперативной группы.

Необходимо четко организовать поисковые мероприятия, направленные на поиск тайников, в которых могут находиться предметы, устройства и документы. Ими могут быть и сами СКТ – аппаратные и программные оболочки модулей, их составляющих.

На заключительном этапе обыска составляются протокол следственного действия и описи к нему; вычерчиваются планы обыскиваемых помещений, схемы расположения ИТ-техники относительно друг друга, строительных проемов, инженерно-технических коммуникаций, оконечных устройств электронесущей арматуры, а также принципиальная схема соединения ИТ-аппаратуры между собой и с другими техническими устройствами; проводятся дополнительная фотосъемка и видеозапись.

Предметом выемки в абсолютном большинстве случаев являются: средства ИТ-техники; электронные носители информации, компьютерная информация; всевозможные документы; средства защиты информации; специальная разведывательная и контрразведывательная аппаратура, в том числе средства подавления радиосигналов и постановки радиопомех; свободные образцы почерка, печатных текстов и готовой продукции для сравнительного исследования.

Помимо вышеуказанного изъятию подлежат материалы, предметы, приспособления, устройства и инструменты, которые могли быть использованы преступником при изготовлении орудий преступления, поддельных документов, электронных носителей информации и самой компьютерной информации; черновики, на которых отрабатывалась поддельная подпись или другие реквизиты документа; копии и бланки регистрационно-учетных документов и расчетно-кассовых операций; техническая и справочная литература, косвенно связанная с технологией обращения и изготовления электронных документов и электронных носителей информации, орудий преступления; фотографии, аудио-, видеоносители с записями соответствующего содержания, в том числе с зарубежными художественными видеофильмами, содержащими эпизоды преступной деятельности, способы подготовки, совершения и сокрытия преступлений, изготовления спецтехники; оргтехника (копировальные и печатные аппараты); штампы, печати и маркираторы; ламинаторы; средства нанесения защитных знаков и т. д.

Особо следует остановиться на изъятии мобильных телефонов и иных средств телекоммуникационной техники[1]. Данные устройства, так же как и иные электронные носители, изымаются в соответствии с требованиями ч. 2 ст. 164.1 УПК РФ, т. е. с обязательным участием специалиста и понятых. Поиск мобильных устройств в ходе обыска может осуществляться

[1] Родивилина В. А., Цуканов Н. Н. Изъятие и осмотр мобильного телефона как электронного носителя информации // Вестник Восточно-Сибирского института МВД России. 2019. № 4 (91). С. 107–114.

с применением специальной сканирующей аппаратуры. По возможности следует обнаружить и изъять зарядное устройство, техническую документацию (паспорт) и договор с предоставляющим услуги связи оператором (PIN-коды для SIM-карт). Информация, которую владелец (или иное лицо) сообщил, включая коды доступа к устройству, фиксируется как объяснение или собственноручно написанное заявление. В протоколе указываются марка, характерные признаки мобильного средства, его состояние (включено или выключено, заблокировано или нет). Как уже отмечалось, мобильное устройство следует немедленно перевести в авиарежим либо иным способом сделать недоступным для управляющих команд извне. В противном случае с помощью команд удаленного доступа содержащаяся на нем информация может быть удалена либо модифицирована без возможности ее восстановления. По окончании изъятия мобильного устройства ему необходимо обеспечить электропитание до поступления телефона в экспертное учреждение, в противном случае батареи через непродолжительное время разрядятся, и упаковать по общим правилам упаковки СКТ.

Состояние изъятых в ходе обыска (выемки) средств компьютерной техники, информационно-телекоммуникационного оборудования, электронных носителей информации и других предметов отображается в протоколе соответствующего следственного действия, при необходимости сопровождается фото- / видеофиксацией. При этом фиксируются только внешние признаки. Тщательное исследование изъятых объектов лучше проводить в ходе компьютерной (компьютерно-технической) экспертизы либо (в крайнем случае) самостоятельного осмотра с участием специалиста и понятых.

Например, участники специально созданной организованной преступной группы получили в свое распоряжение и пользование компьютерные программы, позволяющие считывать информацию о состоянии кассет банкомата (наличие и количество купюр) и управлять диспенсером банкомата путем отправки команд на выдачу денежных купюр в любом доступном объеме. Затем один из соучастников скомпрометировал (то есть получил возможность неправомерно использовать) локальную сеть АКБ «А.» и осуществил сетевые атаки, направленные на реализацию удаленного контроля над ПК сотрудников банка, в конечном итоге получил доступ к банкоматам АКБ «А.», откуда другие соучастники снимали денежные средства. В ходе проведения обыска в жилище одного из соучастников, Л., были добровольно выданы видеорегистратор, блок питания, мышь, платежные документы, чеки, ноутбук, шесть симкарт, банковская карта, два сотовых телефона и другие предметы и документы. В ходе обыска в жилище другого соучастника, З., были изъяты мобильные телефоны, деньги и другие предметы и документы, а также USB-накопитель. Последующим осмотром изъятого USB-накопителя было установлено, что на нем имеется информация, касающаяся

деятельности сервисов сети Интернет, связанных с обменом электронных денежных средств. Осмотр ноутбука позволил установить переписку участников преступной группы[1].

Следователю нужно быть особенно внимательным при использовании специальной терминологии. Внешний вид устройства не всегда позволяет точно его установить. Так, небольших размеров устройства с USB-разъемом часто называют USB-флэш-накопителями или просто «флэшками». Это может быть действительно так, но подобный внешний вид может иметь и другое оборудование, например, телекоммуникационное. Соответствующие надписи на корпусе от длительного использования иногда стираются, что еще больше затрудняет точное определение типа устройства. Поэтому при описании таких объектов лучше употреблять общие термины, например «USB-устройство».

Расследование преступлений, совершенных с использованием ИТТ, нередко требует получения информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ). Такая информация может потребоваться, например, для установления лиц, причастных к совершению преступления[2]. Хотя данное следственное действие с уголовно-процессуальной точки зрения не является изъятием электронных носителей и компьютерной информации, в тактико-криминалистическом аспекте оно имеет определенное сходство с их выемкой. Информация о соединениях, как правило, формируется в автоматическом режиме, хранится в осуществляющей услуги связи организации в электронном виде и предоставляется следователю на бумажном носителе, а в случае значительного объема – на электронном.

В производстве рассматриваемого следственного действия традиционно выделяется три этапа.

Первый этап – подготовительный. На этом этапе следователь принимает решение о необходимости получения информации о соединениях между абонентами и (или) абонентскими устройствами. Решение о том, что такие сведения имеют значение для уголовного дела, является во многом субъективным и зависит от следователя, его опыта, уже имеющейся информации по делу, следственных версий и других факторов. Аргументами можно считать способ совершения преступления, заключающийся в передаче информации с помощью средств связи (выдвижение

---

[1] Уголовное дело № 1-681/2022 Якутского городского суда Республики Саха (Якутия) // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

[2] Дерюгин Р. А. Получение информации о соединениях между абонентами и (или) абонентскими устройствами в структуре тактической операции по установлению лиц, причастных к совершению преступления // Вестник Восточно-Сибирского института МВД России. 2018. № 3 (86). С. 178–184.

требований потерпевшему, распространение запрещенной информации, неправомерный доступ к компьютерной информации и т. п.) либо в хищении абонентских устройств, и сведения, что во время совершения преступления, а равно непосредственно перед ним или после него преступник пользовался услугами связи. Запрос может быть осуществлен в целях установления контактов подозреваемого, в том числе с возможными соучастниками, проверки алиби и т. д. Сведения о соединении между абонентскими устройствами могут использоваться и для преодоления противодействия расследованию уголовного дела. Также следователю необходимо определить, какая информация представляет интерес для расследования. Как правило, это дата, время начала и окончания соединения, его продолжительность (объем предоставленной услуги), номера абонентов (ч. 5 ст. 186.1 УПК РФ), тип соединения (входящий/исходящий), вид предоставляемых услуг (телефонное соединение, SMS/EMS/MMS, подключение к информационно-телекоммуникационной сети Интернет), номер базовой станции, позволяющий установить примерное местонахождение абонентского устройства (геолокация), и т. д.

Важно определиться с периодом получения информации. Это могут быть сведения как об уже совершенных соединениях (ретроспективный аспект), так и о предстоящих (перспективный аспект). При этом сведения о состоявшихся соединениях могут запрашиваться за любой период, который ограничивается только относимостью к расследуемому уголовному делу, соображениями разумности и техническими возможностями оператора связи предоставить такую информацию. Перспективный период, в соответствии с частями 4, 7 статьи 186.1 УПК РФ, ограничен сроком до шести месяцев, но не позднее окончания предварительного расследования по уголовному делу.

На этом же этапе необходимо установить оператора связи, предоставляющего соответствующие услуги абоненту. В информационно-телекоммуникационной сети Интернет существует довольно много различных сервисных программ, позволяющих по абонентскому номеру установить оператора связи и регион, в котором этот номер зарегистрирован. Однако к таким сведениям следует относиться с определенной критичностью. В частности, они не всегда отображают факт перенесения абонентских номеров при смене оператора в соответствии со статьями 26, 46 ФЗ «О связи». Поэтому, прежде чем производить следственное действие, целесообразно направить в организацию (организации) связи запрос, является ли интересующее следствие лицо их абонентом (обслуживается ли ими указанный абонентский номер). Ответ на такой запрос содержит только сведения о наличии либо отсутствии регистрации абонента и (или) абонентского устройства, поэтому его направление не требует судебного решения. Данная информация может быть получена и оперативным путем, поскольку ее назначение – ориентирующее.

Вторым пунктом подготовительного этапа получения информации о соединениях будет возбуждение следователем перед судом ходатайства о производстве следственного действия, о чем выносится постановление в порядке, предусмотренном статьей 165 УПК РФ. В соответствии с ч. 2 ст. 165 УПК РФ, ходатайство о производстве такого следственного действия подлежит рассмотрению единолично судьей районного суда по месту производства предварительного следствия или производства следственного действия. Однако, как свидетельствует практика, независимо от места расположения органа, осуществляющего расследование, ходатайство следует подавать в суд по месту совершения преступления (если оператор связи находится в другом регионе) либо по месту производства следственного действия.

Определившись с подсудностью рассмотрения материалов, следователь приступает к составлению текста ходатайства, как это предписывается ч. 2 ст. 186.1 УПК РФ. И если указать уголовное дело (номер, дату возбуждения, статьи УК РФ и (при наличии) лицо, в отношении которого производится расследование), период (ретроспективный), за который требуется получить информацию, и (или) срок (перспективный) производства следственного действия, а также наименование организации (оператора связи), предоставляющей сведения, как правило, не вызывает затруднений, то привести основания, по которым необходимо получить информацию о соединениях между абонентами и (или) абонентскими устройствами, является, пожалуй, самой сложной частью следственного действия. Особенно это касается возможности получения информации в отношении неопределенного круга лиц, в частности сведений о соединениях между абонентами и абонентскими устройствами, которые выходили на связь (были активны) в месте совершения преступления через базовые станции операторов сотовой связи, осуществляющих уверенное покрытие по указанному адресу в заданный период времени, поскольку ставятся под угрозу права неопределенного числа граждан на тайну телефонных переговоров, что противоречит требованиям ст. 23 Конституции Российской Федерации и ст. 13 УПК РФ. Однако подобные запросы в сочетании с использованием специализированных аппаратно-программных комплексов являются эффективным способом раскрытия и формирования доказательственной базы по некоторым категориям преступлений.

Помимо перечисленных в части 2 статьи 186.1 УПК РФ пунктов в ходатайстве также следует указать номера абонентов и (или) абонентских устройств, адрес, на который оператор связи должен будет представить информацию, и характер этой информации (дата, время и длительность, тип соединения, номера абонентов и (или) абонентских устройств, номера и местонахождение базовых станций и т. д.). Для подключения абонентского устройства к сети Интернет помимо времени и продолжи-

тельности использования трафика важным показателем является объем принятой и переданной информации.

Третьим, завершающим, пунктом подготовительного этапа выступает рассмотрение ходатайства судом. Участие следователя на данном этапе опосредованное. Он вправе присутствовать при рассмотрении своего ходатайства и давать необходимые пояснения. В частности, следователь должен обращать внимание на то, чтобы разрешение ходатайства осуществлялось в закрытом судебном заседании и в постановлении имелось соответствующее указание. Копию полученного судебного решения следователь направляет оператору связи для исполнения.

Рабочим этапом данного следственного действия будет получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами, ее изучение и приобщение к материалам уголовного дела. Информация может представляться как на бумажных носителях, так и в электронном виде. Последнее характерно для значительных массивов данных, кроме того, для возможности автоматизированной обработки информации такой вариант предпочтительнее.

Осмотр полученной информации во многом схож с осмотром документов, регламентированным статьей 177 УПК РФ. Вместе с тем он является частью следственного действия, предусмотренного статьей 186.1 УПК РФ, а потому имеет свои особенности[1]. В частности, в соответствии с ч. 2 ст. 170 УПК РФ, следователь самостоятельно принимает решение о необходимости участия понятых, но при их отсутствии применение технических средств фиксации хода и результатов следственного действия не является обязательным.

Участие в осмотре специалиста не является обязательным, но оно целесообразно, когда необходимо исследовать значительный массив информации (например, сведения об активных абонентских устройствах в месте совершения преступления). Необходимость его привлечения также определяется следователем (ч. 5 ст. 186.1 УК РФ).

По существу, именно доказательства, полученные в ходе осмотра представленной информации, являются целью данного следственного действия. Например, в ходе расследования уголовного дела по обвинению Л. в совершении двух покушений на незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, группой лиц по предварительному сговору, в особо крупном размере (ч. 3 ст. 30, ч. 5 ст. 228.1 УК РФ)

[1] Варданян А. В., Цыкора А. А. Правовая природа и тактико-криминалистические особенности производства следственных действий, связанных с получением и анализом информации о телекоммуникационных соединениях между абонентами и (или) абонентскими устройствами // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 25.

была получена информация о соединениях абонентского номера, принадлежащего обвиняемому, в бумажном виде на 23 страницах. Проведенным осмотром было установлено, что в представленной таблице имеются столбцы с информацией о совершении телефонных и иных соединений с использованием указанного абонентского номера, сведения об абоненте, на которого зарегистрирован данный номер, а также информация о периоде полученной детализации. На последующих листах в табличном виде представлена интересующая следствие информация о входящих/исходящих соединениях абонентского номера Л. с указанием даты, времени и номера телефона собеседника. Из информации следовало, что первые телефонные соединения Л. с другими лицами, которые были приняты базовыми станциями оператора сотовой связи, совпадают с местом и временем осуществления Л. закладок наркотических средств, что подтвердило его показания, данные в ходе допроса[1].

На заключительном этапе следователь составляет протокол о проведенном осмотре, руководствуясь требованиями статьи 166 УПК РФ. Вне зависимости от того, имеет представленная информация отношение к уголовному делу или нет, все полученные от осуществляющей услуги связи организации документы должны на основании постановления следователя быть признаны вещественными доказательствами, приобщены к материалам уголовного дела в полном объеме и храниться в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

Очевидно, что в случае, когда в течение срока производства следственного действия осуществляющая услуги связи организация неоднократно предоставляет информацию о соединениях, следователь обязан производить осмотр этой информации по мере ее поступления, каждый раз действуя в соответствии с частями 5, 6 статьи 186.1 УПК РФ.

В заключение еще раз отметим, что производство следственных действий, направленных на изъятие электронных носителей информации и компьютерной информации, требует от следователя не только строгого соблюдения уголовно-процессуальных норм, но и выполнения технико-криминалистических рекомендаций, отступление от которых с большой вероятностью может привести к уничтожению или искажению цифровых следов, что в конечном итоге влечет признание доказательств недопустимыми.

---

[1] Уголовное дело № 1-107/2020 Дзержинского районного суда г. Волгограда Волгоградской области // Судебные и нормативные акты Российской Федерации : сайт. URL: https://sudact.ru/.

Контрольные вопросы

1. Какие процессуальные требования предъявляются к изъятию электронных носителей информации?
2. Какие мероприятия необходимо осуществить следователю на подготовительном этапе обыска по преступлениям, совершенным с использованием ИТ-технологий?
3. Назовите тактико-криминалистические особенности производства обыска по преступлениям, совершенным с использованием ИТ-технологий.
4. Как производится изъятие устройств мобильной связи?
5. Назовите тактико-криминалистические особенности получения информации о соединениях между абонентами и (или) абонентскими устройствами при расследовании уголовных дел по преступлениям, совершенным с использованием ИТТ.

§ 5. Назначение судебных экспертиз при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Использование специальных знаний вносит весомый вклад в формирование доказательственной базы при расследовании преступлений, совершенных с использованием ИТ-технологий.

Специальные знания – это система теоретических знаний, практических навыков в области конкретной науки, техники, искусства, ремесла, приобретаемых путем специальной подготовки и профессионального опыта и необходимых для решения вопросов, возникающих в процессе уголовного, гражданского, административного судопроизводства[1].

Самым результативным видом процессуальной формы использования специальных знаний является судебная экспертиза[2].

Основной целью судебной экспертизы является получение объективной и достоверной информации, которая может быть использована в суде в качестве самостоятельного доказательства. В контексте преступлений, совершенных с использованием ИТТ, судебная экспертиза может применяться для установления лиц, причастных к этим преступлениям, а также для восстановления цифровых доказательств, которые могли быть утеря-

---

[1] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе : монография / 4-е изд. М., 2018. С. 5.

[2] Усачев С. И. Особенности использования специальных знаний при расследовании мошенничества в сфере автострахования : дис. … канд. юрид. наук. Калининград, 2022. С. 130.

ны, уничтожены или спрятаны преступниками. Благодаря беспристрастности и достоверности результаты судебной экспертизы представляют собой ценные доказательства, которые могут быть использованы в суде для подтверждения или опровержения какого-либо факта.

УПК РФ регламентирует порядок назначения, производства и оценки заключений судебных экспертиз (см. рис. 19).

В 2021 году в постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам»[1] внесены дополнения, указывающие на недопустимость постановки эксперту вопросов, связанных с оценкой достоверности показаний подозреваемого, обвиняемого, потерпевшего или свидетеля, полученных в ходе производства допроса, очной ставки и иных следственных действий, в том числе с применением аудио- или видеозаписи, поскольку такая оценка, в соответствии со ст. 88 УПК РФ, относится к исключительной компетенции лиц, осуществляющих надзор и производство по уголовному делу.

При ознакомлении с постановлением о назначении экспертизы реализовывается право участников уголовного судопроизводства заявить об отводе эксперта либо о возможности проведения экспертизы в ином экспертном учреждении. Данное право закреплено в пп. 2 п. 1 ст. 198 УПК РФ,

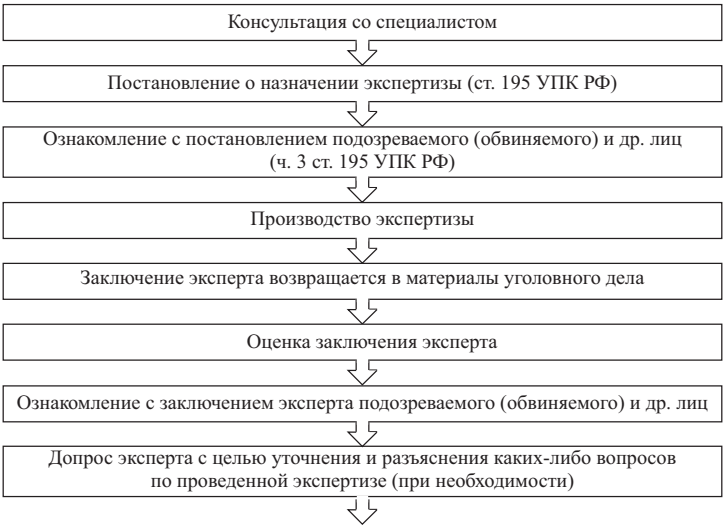


Рис. 19. Этапы назначения, производства и оценки заключений судебных экспертиз

[1] О судебной экспертизе по уголовным делам : постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_108437/.

также на необходимость его обеспечения указано в п. 3 постановления Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам».

Так, назначая экспертизу, следователь выносит об этом постановление, с которым знакомит подозреваемого (обвиняемого), чем обеспечивает соблюдение упомянутых выше прав. Однако изучение судебной и следственной практики позволяет сделать вывод о том, что не всегда следователь действует в соответствии с требованиями закона. Нередко ознакомление с постановлением о назначении экспертизы проводится параллельно с ознакомлением с заключением эксперта. По данному поводу Конституционный Суд Российской Федерации дает пояснения, заключающиеся в том, что при установлении подобных фактов подозреваемый (обвиняемый) имеет право обратиться с жалобой в прокуратуру или суд, а также требовать проведения дополнительной или повторной экспертизы[1]. Указанные нарушения могут повлечь за собой отмену приговора или его изменение.

Одним из самых распространенных экспертных исследований, проводимых при расследовании преступлений, совершенных с использованием ИТТ, является судебная компьютерная экспертиза. Следует отметить, что в системе МВД России данный род исследования имеет наименование «компьютерная экспертиза», а вид исследования – «исследование компьютерной информации»[2]. В экспертных подразделениях Минюста России используют понятия «компьютерно-техническая экспертиза» и «исследование информационных компьютерных средств»[3]. В эксперт-

---

[1] По жалобе гражданина Алеева Руслана Ильгизаровича на нарушение его конституционных прав положениями статей 195 и 198 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда Российской Федерации от 5 февраля 2015 г. № 259-О // КонсультантПлюс : сайт. URL: http://172.30.6.144/cons/cgi/online.cgi?req=doc&base=ARB&n=419645&cacheid=6FC8E2F9B5862FEBBE6D6185084FDCEA&mode=splus&rnd=NuGX84UEF2Cfwr671#7CQX84UUHC1vS3Iq.

[2] Перечень родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации : Приложение № 2 к приказу МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_55315/171f22ad9900f6b9d88242eab4a97f23c815fb19/.

[3] Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России : приказ Минюста России от 27 декабря 2012 г. № 237 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_141682/.

ных подразделениях ФСБ России, согласно нормативным документам, данные исследования носят наименование «компьютерные экспертизы» с перечнем видов проводимых исследований:

1) обеспечение доступа к информации, содержащейся в компьютерах и на компьютерных носителях информации;

2) определение назначения и функциональных возможностей программного обеспечения и компьютерных устройств;

3) выявление действий, произведенных с компьютером и хранящейся в нем информацией[1].

В Судебно-экспертном центре СК России используется формулировка «компьютерно-техническая экспертиза», специальность «Исследование цифровой информации и компьютерных средств»[2]. Согласно действующему стандарту ГОСТ Р 57429-2017[3], данный род экспертиз носит название «судебная компьютерно-техническая экспертиза».

Так как наибольшее количество уголовных дел, связанных с использованием ИТТ, с учетом подследственности, определенной в ст. 151 УПК РФ, расследуется в подразделениях МВД России, то и экспертизы в отношении компьютерных устройств по этим уголовным делам чаще всего проводятся в экспертно-криминалистических подразделениях органов внутренних дел. В таких случаях должно использоваться наименование судебной экспертизы, приведенное в Перечне родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, утвержденном приказом МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», – компьютерная экспертиза. Кроме того, предмет судебной компьютерно-технической экспертизы шире, чем компьютерной экспертизы.

Существуют различные типы цифровых доказательств, которые могут быть обнаружены или восстановлены в ходе судебной компьютерной экспертизы, в том числе:

---

[1] Об утверждении Положения об экспертных подразделениях в органах федеральной службы безопасности : приказ ФСБ России от 31 января 2002 г. № 60 (текст приказа официально опубликован не был).

[2] Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации» на право самостоятельного производства судебных экспертиз : приказ СК России от 24 июля 2020 г. № 77 // Кодификация РФ. Действующее законодательство Российской Федерации : сайт. URL: https://rulaws.ru/acts/Prikaz-SK-Rossii-ot-24.07.2020-N-77/.

[3] ГОСТ Р 57429-2017. Судебная компьютерно-техническая экспертиза. Термины и определения. М. : Стандартинформ, 2018.

– файлы и данные компьютеров и мобильных устройств;

– электронная почта и информация, содержащаяся в системах мгновенного обмена сообщениями;

– интернет-активность и данные веб-сайта;

– активность (действия) лица и его посты в социальных сетях;

– электронные финансовые транзакции.

Далее укажем объекты, которые можно направить на судебную компьютерную экспертизу:

– системные блоки персональных компьютеров, ноутбуки, нетбуки, макбуки и т. д.;

– машинные носители информации (накопители на жестких магнитных дисках, твердотельные накопители, флеш-накопители, карты памяти, оптические диски и т. д.);

– мобильные телефоны, смартфоны, планшетные компьютеры, SIM-карты;

– видеорегистраторы;

– платежные пластиковые карты;

– майнинговое оборудование.

При вынесении постановления о назначении компьютерной экспертизы для сокращения объемов, сроков проведения экспертизы и получения ожидаемых результатов необходимо формулировать вопросы по существу, т. е. таким образом, чтобы было понятно, какую информацию или следы каких действий необходимо обнаружить. В связи с индивидуальными особенностями каждой назначаемой экспертизы необходимо предварительно проконсультироваться с экспертом для грамотного формулирования вопросов, выносимых на экспертизу.

Для доступа к содержимому мобильных телефонов (смартфонов) сотрудникам экспертных подразделений часто требуются пин-коды либо графические пароли, которые установлены на предоставляемых устройствах. Данные пароли не всегда могут быть подобраны силами экспертов, поэтому рекомендуется при наличии информации о паролях предоставляемых устройств (даже при наличии информации о части пароля либо о количестве символов в пароле) указывать данную информацию при проведении осмотров и назначении экспертиз. Кроме того, поскольку исследование информации, содержащейся в мобильных телефонах, планшетах, макбуках, как правило, проводится при включенном компьютерном устройстве, необходимо, чтобы в постановлении о назначении компьютерной экспертизы содержалось разрешение на использование видоизменяющих методов исследования.

Упаковка компьютерной техники и носителей информации, представляемых на экспертизу, должна содержать оттиски печати и необходимые пояснительные надписи, не иметь повреждений и исключать возможность доступа к содержимому без нарушения ее целостности. Компью-

терная техника, представляемая на экспертизу в неупакованном виде, должна иметь неповрежденные оттиски печати. В случае обнаружения повреждений упаковки или оттисков печати, а также признаков вскрытия эксперт должен зафиксировать указанные обстоятельства в заключении. Этот факт может негативно отразиться на дальнейшем ходе расследования и послужить отправной точкой для оказания противодействия расследованию со стороны подозреваемого (обвиняемого) и стороны защиты.

Проведенное авторами настоящего пособия интервьюирование сотрудников экспертных учреждений позволило структурировать и обобщить рекомендации по постановке вопросов, выносимых на экспертизу.

В первую очередь вопросы, выносимые на компьютерную экспертизу, должны удовлетворять определенным требованиям, которые можно разделить на две группы: общие требования, которые можно отнести к любым вопросам, выносимым на компьютерную экспертизу, и частные требования, относящиеся к вопросам, выносимым на экспертизу по конкретному расследуемому событию, которые определены в разработанной типовой методике компьютерной экспертизы[1].

Общие требования:

1. При постановке вопроса необходимо использовать лексику, исключающую жаргонные и полупрофессиональные термины («винчестер» – НЖМД, «логи» – протоколы, «логин» – имя пользователя и т. п.), закрепленную в соответствующих ГОСТах или употребляемую разработчиками технических средств, программных продуктов в документации, описаниях, справках и т. п.

2. Вопрос должен быть четким и однозначным.

3. Формулировка вопроса не должна касаться этапов исследования информации.

4. Вопрос не должен носить справочный характер, ответ на него должен требовать применения специальных знаний (получить разъяснения о том, что может означать тот или иной термин, интерпретировать информацию и прочее можно в рамках других следственных действий, позволяющих специалисту высказывать свое мнение).

5. Вопрос не должен носить правовой характер и выходить за пределы компетенции эксперта.

6. Вопрос должен соответствовать существующей методической и технической базе.

Частные требования:

1. Вопросы должны быть направлены на установление конкретных обстоятельств расследуемого события.

---

[1] Саенко Г. В., Тушканова О. В. Компьютерная экспертиза // Типовые экспертные методики исследования вещественных доказательств. Ч. I / под ред. канд. техн. наук Ю. М. Дильдина; общ. ред. к.т.н. В. В. Мартынова. М., ЭКЦ МВД России, 2010. С. 199.

2. Вопросы должны быть поставлены так, чтобы при решении конкретных задач расследования затраты (финансовые, технические, временные) на проведение исследований были минимальными.

3. Вопросы должны соответствовать уровню подготовки и инструментальному оснащению экспертов того экспертного учреждения, в которое направляется экспертиза.

4. Вопросы должны соответствовать представляемым на исследование объектам[1].

Основные возможности компьютерной экспертизы:

– поиск графических, текстовых файлов по заданным ключевым словам и фразам;

– поиск аудио-, видео- и других типов файлов;

– поиск программных продуктов и регистрационных данных, указанных в этих продуктах (ключ продукта, версия продукта, имя пользователя), а также возможность их запуска на ПК;

– поиск программных продуктов (генераторов ключей, патчеров, активаторов), позволяющих обойти средства защиты авторских прав программ-правообладателей, например «Microsoft», «Autodesk»;

– поиск сведений об обстоятельствах, интересующих следствие;

– поиск сетевых настроек предоставляемых устройств (например, определение внутреннего локального IP-адреса системного блока, а не внешнего, который предоставляется провайдером);

– выявление метаданных файлов (дата создания, последнего изменения файла, номер версии или редакции, название организации или компании, имя компьютера, имя сервера в сети или диск, имена авторов и т. п.);

– поиск электронной почтовой переписки, в том числе в программах мгновенного обмена сообщениями (WhatsApp, Viber, Telegram и т. п.);

– поиск посещенных интернет-ресурсов;

– выявление сведений об установленных приложениях, программах и результатах их работы;

– проверка наличия и анализ программ, определяемых антивирусным программным обеспечением как «троянские»;

– извлечение файлов видеозаписей с камер видеонаблюдения, видеорегистраторов;

– считывание информации с магнитных полос пластиковых карт;

– определение IMEI телефона и проверка соответствия его значения, содержащегося в памяти телефона, нанесенному на корпус телефона или содержащемуся в документации к нему;

– поиск в памяти мобильного телефона информации, вводимой абонентом (номера телефонов, смс-сообщения и другая), и информации,

[1] Муленков Д. В. Особенности назначения судебно-компьютерных экспертиз // Криминалистика: вчера, сегодня, завтра. 2015. Выпуск 6. С. 154–161.

накопленной в телефоне при его работе в сети сотовой связи (последние набранные и полученные звонки, принятые сообщения);

– поиск баз данных и сведений о зарегистрированных в них организациях (например, 1С);

– восстановление удаленной информации на мобильных устройствах, персональных компьютерах и иных носителях информации;

– обход паролей пользователей операционных систем «Windows», «MacOS», некоторых мобильных устройств, пользователей баз данных программы «1С:Предприятие»;

– извлечение сведений из майнингового оборудования, таких как MAC-адрес, интернет-ссылка пула (майнинг-пул – это сервер, который делит большую задачу по вычислению подписи блока на маленькие задачи и раздает их подключенным устройствам; пул – это объединение мощности оборудования сразу многих майнеров для повышения вероятности нахождения блока; награда за блок, добытый пулом, распределяется среди всех участников[1]), имя воркера (от англ. worker – работник, имя майнингового оборудования, которое используют как логин для майнингового программного обеспечения);

– восстановление удаленной информации на машинных носителях (НЖМД, SSD и т. д.);

– обход средств защиты (паролей, пин-кодов) пользователей ПК.

Если необходимо провести на машинном носителе (в средстве вычислительной техники) поиск информации, созданной с помощью прикладных программ, либо сведений о действиях пользователя, то перед экспертом ставятся вопросы[2]:

1. Находится ли объект исследования в рабочем состоянии?

2. Имеется ли на представленных объектах (дать перечень объектов) информация, содержащая следующие ключевые слова: (дать перечень ключевых слов)?

3. Имеется ли на представленных объектах (дать перечень объектов) информация о (изложить, о чем)?

Определенную специфику имеет решение задач по поиску и интерпретации информации, содержащейся в мобильных телефонах.

Перед экспертом могут быть поставлены вопросы:

1. Имеется ли в представленном на экспертизу мобильном телефоне, установленных в нем SIM-карте и карте памяти информация, вводимая

---

[1] Багнюк М. Р. Саморегулирующиеся организации и необходимость их законодательного закрепления (на примере mining pool) // Право. Общество. Государство : сб. науч. тр. студентов и аспирантов / отв. ред. Е. В. Трофимов. Том 7. Санкт-Петербург : Санкт-Петербургский институт (филиал) ВГУЮ (РПА Минюста России), 2019. С. 187–191.

[2] Саенко Г.В., Тушканова О. В. Компьютерная экспертиза // Типовые экспертные методики исследования вещественных доказательств. Ч. I. М., 2010. С. 189.

абонентом (номера телефонов (телефонная книга), SMS-сообщения, аудио-, видео- и графические файлы и др.), и информация, накопленная в телефоне при его работе в сети сотовой связи (последние набранные и полученные звонки, принятые сообщения и др.)? Если да, то какая?

2. Каково значение IMEI, содержащегося в памяти представленного мобильного телефона?

3. Соответствует ли значение IMEI, содержащегося в памяти представленного мобильного телефона, значению IMEI, нанесенного на... (корпус, упаковку, этикетку и пр.)?

4. Имеется ли на представленном объекте информация о выходе в сеть Интернет за период времени с ... по ...? Если да, то на какие интернет-ресурсы?

5. Имеется ли на представленном объекте информация о выходе в сеть Интернет на интернет-ресурс (например, avito.ru) в период времени с ... по ...?

6. Имеется ли на представленном объекте электронная переписка в период с ... по ...?

7. Имеется ли на представленном объекте электронная переписка в приложениях, например «WhatsApp», в чате «указать наименование» за период с ... по ...?

8. Имеются ли на представленном объекте программы, определяемые антивирусным программным обеспечением как «трояны»?[1]

При исследовании информации, содержащейся на магнитной полосе платежных/пластиковых карт, перед экспертом могут быть поставлены следующие вопросы:

1. Какая информация имеется на магнитной полосе пластиковой карты, представленной на исследование?

2. Соответствует ли информация, записанная на магнитную полосу пластиковой карты, информации, имеющейся в элементах внешнего оформления данной карты?

3. Может ли представленная на исследование пластиковая карта быть воспринята в технологии функционирования платежной системы в качестве платежной (при условии использования информации, записанной на магнитную полосу карты) на определенную дату или период времени?[2]

Радиотехническая экспертиза.

Сущность РТЭ заключается в проведении исследования технических средств различного назначения, представляющих собой устройства для

---

[1] Типовая методика исследования информации в мобильных телефонах / О. В. Тушканова и др. М., 2014. С. 9.

[2] Саенко Г.В., Тушканова О. В. Компьютерная экспертиза // Типовые экспертные методики исследования вещественных доказательств. Ч. I. М., 2010. С. 237.

передачи, приема, преобразования и обработки информации с использованием электромагнитных колебаний и электронных процессов в различных средах.

Объектами РТЭ являются радиотехнические изделия (комплекты и комплексы из них) или их фрагменты, отдельные компоненты, комплектующие и содержащаяся в них информация (например, брелоки автомобильных сигнализаций, блокираторы связи, программаторы, средства для скрытного прослушивания и видеонаблюдения и т. д.).

Основные направления, по которым проводятся РТЭ:

– исследование специальных технических средств для несанкционированного получения конфиденциальной клиентской информации из систем дистанционного банковского обслуживания (скимминг);

– исследование специальных технических средств для несанкционированного отключения охранных систем автотранспорта;

– исследование исполнительных механизмов самодельных взрывных устройств;

– исследование специальных технических средств для негласного получения информации.

Порядок изъятия рассматриваемых устройств регламентируется уголовно-процессуальным законодательством (ст. 164.1 УПК РФ).

На экспертизу необходимо при наличии возможности представить пароли, пин-коды, графические ключи либо комбинации нажатия кнопок управления на брелоке автосигнализации (которые активируют какие-либо функции).

Если устройство было включено, то необходимо по возможности обеспечить его предоставление на экспертизу во включенном состоянии. При его направлении на экспертизу об этом обязательно уведомляется эксперт.

При исследовании радиоэлектронного оборудования, используемого при хищениях транспортных средств, применяются методы, сопряженные с демонтажем их корпусов. Нередко изготовители такого оборудования используют различные компаунды и клеи, препятствующие применению подобного рода методов без возможных изменений внешнего вида и конструктивных свойств исследуемого объекта. При вынесении постановлений о назначении судебных экспертиз следует учитывать данные обстоятельства и разрешать эксперту при производстве экспертизы совершать необходимые действия, сопряженные с изменениями внешнего вида и конструктивных свойств. В постановлении о назначении радиотехнической судебной экспертизы следует указать: «Разрешаю применение видоизменяющих (разрушающих) методов исследования».

Таким образом, очевидно, что в случаях, когда речь идет о преступлениях, совершаемых с использованием ИТ-технологий, практически всегда назначаются и проводятся различные судебные экспертизы.

Безусловно, наиболее актуальными являются судебные компьютерно-технические и радиотехнические экспертизы, так как именно они позволяют получить ответы на достаточно сложные вопросы, касающиеся возможностей рассматриваемых технологий. Однако следует учитывать тот факт, что зачастую уровень знаний, умений и навыков преступников значительно превосходит опыт сотрудников правоохранительных органов, что требует от последних постоянного профессионального совершенствования.

Контрольные вопросы

1. Что является основной целью судебной экспертизы?
2. Каков порядок назначения и производства судебных экспертиз по уголовным делам о преступлениях, совершенных с использованием ИТТ?
3. Виды экспертиз, проводимых при расследовании преступлений, совершенных с использованием ИТТ?
4. Какие объекты можно направить на судебную компьютерно-техническую экспертизу?
5. Каковы рекомендации по постановке вопросов, выносимых на экспертизу по уголовным делам о преступлениях, совершенных с использованием ИТТ?

ЗАКЛЮЧЕНИЕ

Глобальная цифровизация и информатизация всех сфер жизни человека дает огромные преимущества человечеству, перечислить которые полностью не представляется возможным. Функциональные возможности, в том числе по анонимизации лиц, использующих информационные технологии, делают их привлекательными для преступной сферы. Распространенность преступлений, совершаемых с использованием информационных технологий, приобретает угрожающие масштабы, о чем свидетельствует приведенная статистика.

Ежегодно на расширенных заседаниях коллегий МВД России Президент Российской Федерации Путин В. В. обращает внимание на рост преступности с использованием ИТТ и ставит перед ведомством задачи, в том числе осуществление эффективной деятельности по противодействию преступлениям в рассматриваемой сфере посредством применения современного технико-криминалистического и тактического инструментария.

Практическая потребность в данном инструментарии определила направление развития теоретических положений обеспечения криминалистической деятельности. Осуществленные в рассматриваемой сфере исследования позволили запустить процесс формирования частной теории информационно-технологического обеспечения криминалистической деятельности. Однако временем для формирования учения располагает только теория, а правоприменительная деятельность уже сегодня нуждается в сформированных рекомендациях правового, тактического характера, позволяющих эффективно раскрывать и расследовать преступления, совершенные с использованием ИТТ.

Резюмируя основные положения настоящего пособия, следует отметить:

1. Тенденция к увеличению количества и разнообразия преступлений, совершаемых с использованием информационных технологий, определяет необходимость выработки тактических рекомендаций по проведению отдельных следственных действий. Использование информационных технологий в преступной деятельности кардинально влияет на формирование следовой картины преступления. Цифровые следы имеют специфичную характеристику отображения на носителе, влияющую на возможность их обнаружения, изъятия и сохранения.

2. Знание способов использования информационных технологий в преступной деятельности, их больших возможностей для анонимизации лиц, совершивших преступления, механизма отображения преступной деятельности в компьютерных устройствах и информационном пространстве дает возможность осуществлять поисковую деятельность качественно.

3. Последовательность следственных действий и тактические приемы их проведения определяются с учетом сложившейся следственной ситуации. Основные тактические цели этих следственных действий будут сводиться к установлению электронного носителя информации, обнаружению на нем цифровых следов, их изъятию и дальнейшему исследованию.

4. Тактика производства отдельных следственных действий, таких как следственный осмотр, допросы, обыск и выемка, получение информации о соединениях между абонентами и (или) абонентскими устройствами, имеет специфику. При расследовании преступлений, совершенных с использованием ИТ-технологий, при осмотре места происшествия возникает необходимость применения ч. 3 ст. 177 УПК РФ, закрепляющей возможность осмотра изъятых следов и предметов в ходе самостоятельного следственного действия, поскольку компьютерные устройства являются технически сложными объектами. Содержание и тактика проведения допросов участников уголовного судопроизводства определяются спецификой совершенного преступления. Информированность следователя об обстоятельствах совершенного преступления и его компетентность в рассматриваемых вопросах являются главными составляющими в преодолении противодействия расследованию, которое может быть оказано в ходе допроса. Соблюдение представленных тактических рекомендаций по проведению обыска, выемки и получению информации о соединениях между абонентами и (или) абонентскими устройствами позволит получить криминалистически значимую и доказательственную информацию по уголовному делу.

5. Судебная экспертиза, являясь важным инструментом доказывания, имеет широкие возможности. Одними из распространенных исследований, проводимых при расследовании преступлений, совершенных с использованием ИТТ, являются судебная компьютерная и радиотехническая экспертизы. Соблюдение общих и частных требований к формированию перед экспертами вопросов позволит избежать различных ошибок.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

3. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

4. О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

5. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2007 г. № 149-ФЗ [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

6. О стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

7. О судебной экспертизе по уголовным делам: постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 // [Электронный ресурс] // Доступ из справочно-правовой системы «КонсультантПлюс».

8. 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»: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

9. Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России: приказ МВД России от 11 января 2009 г. № 7 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

10. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с «Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации»): приказ МВД России от 29 июня 2005 г. № 511 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

11. Вопросы определения уровня профессиональной подготовки экспертов в системе МВД России» (вместе с «Положением об аттестации экспертов на право самостоятельного производства судебных экспертиз и о порядке пересмотра уровня их профессиональной подготовки в системе Министерства внутренних дел Российской Федерации», «Положением о Центральной экспертно-квалификаци-

онной комиссии Министерства внутренних дел Российской Федерации»): приказ МВД России от 9 января 2013 г. № 2 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

12. Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России: приказ Минюста России от 27 декабря 2012 г. № 237 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

13. Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации» на право самостоятельного производства судебных экспертиз: приказ СК России от 24 июля 2020 г. № 77 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

14. ГОСТ 15971–1990. Системы обработки информации. Термины и определения: утвержден и введен в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 октября 1990 г. № 2698 / разработан к.т.н. Селивановым Ю. П., Редькиной М. Т., Сергеевой Н. А. – Москва : Издательство стандартов, 1991. – 14 с.

15. ГОСТ Р 56545–2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1180-ст / разработан Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»). – Москва : Стандартинформ, 2015. – 22 с.

16. ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1181-ст / разработан Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»). – Москва : Стандартинформ, 2015. – 17 с.

17. ГОСТ Р 57429–2017. Судебная компьютерно-техническая экспертиза. Термины и определения (Forensic information technology examination. Terms and definitions) : Национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2017 г. № 198-ст : введен впервые : дата введения 2017-09-01. – Москва : Стандартинформ, 2018. – 12 с.

Учебные и научные издания

1. *Алескеров В. И.* Сфера телекоммуникаций и компьютерной информации как платформа для совершения современных видов преступлений : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Л. В. Василенко, С. Н. Ломакин. – Домодедово : ВИПК МВД России, 2021. – 365 с. – Текст : непосредственный.

2. *Багмет А. М.* Цифровые следы преступлений : монография / А. М. Багмет, В. В. Быков, С. Ю. Скобелин. – Москва : Проспект, 2023. – 168 с. – Текст : непосредственный.

3. *Багнюк М. Р.* Саморегулирующиеся организации и необходимость их законодательного закрепления (на примере mining pool) / М. Р. Багнюк. – Текст : непосредственный // Право. Общество. Государство : сборник научных трудов студентов и аспирантов / отв. ред. Е. В. Трофимов. Том 7. – Санкт-Петербург : Санкт-Петербургский институт (филиал) ВГУЮ (РПА Минюста России), 2019. – С. 187–191.

4. *Варданян А. В.* Правовая природа и тактико-криминалистические особенности производства следственных действий, связанных с получением и анализом информации о телекоммуникационных соединениях между абонентами и (или) абонентскими устройствами / А. В. Варданян, А. А. Цыкора. – Текст : непосредственный // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 4-2. – С. 21–26.

5. *Васюков В. Ф.* Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения / В. Ф. Васюков, А. В. Булыжкин. – Текст : непосредственный // Российский следователь. – 2016. – № 6. – С. 3–8.

6. *Гаврилин Ю. В.* Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : учебное пособие / Ю. В. Гаврилин, Г. З. Гаспарян. – Москва : Проспект, 2023. – 128 с. – Текст : непосредственный.

7. *Гаврилин Ю. В.* Противодействие цифровой трансформации наркопреступности (по итогам Всероссийского онлайн-семинара) / Ю. В. Гаврилин. – Текст : непосредственный // Труды Академии управления МВД России. – 2020. – № 4 (56). – С. 122–129.

8. *Грибунов О. П.* Противодействие расследованию преступлений и меры по его преодолению : учебное пособие / О. П. Грибунов, С. В. Унжакова. – Иркутск : ФГКОУ ВО ВСИ МВД России, 2019. – 132 с. – Текст : непосредственный.

9. Зуев С. В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / отв. ред. С. В. Зуев, В. Б. Вехов. – Москва : Издательство Юрайт, 2022. – 243 с. – Текст : непосредственный. 2019. – Текст : непосредственный.

10. *Девяткин Г. С.* Переписка в мессенджерах и социальных сетях как доказательство по уголовному делу / Г. С. Девяткин, П. А. Луценко. – Текст : непосредственный // Государственная служба и кадры. – 2021. – № 2. – С. 159–161.

11. *Дерюгин Р. А.* Получение информации о соединениях между абонентами и (или) абонентскими устройствами в структуре тактической операции по установлению лиц, причастных к совершению преступления / Р. А. Дерюгин. – Текст : непосредственный // Вестник Восточно-Сибирского института МВД России. – 2018. – № 3 (86). – С. 178–184.

12. *Калмыков И. А.* Компьютерная криминалистика : лабораторный практикум / И. А. Калмыков, В. С. Пелешенко. – Ставрополь : Северо-Кавказский федер. ун-т, 2017. – 84 с. – Текст : непосредственный.

13. *Касаев И. Х.* Виктимологическая характеристика преступлений, совершенных с использованием информационно-телекоммуникационных технологий / И. Х. Касаев, К. И. Богомолова, Е. Г. Лиходаев, О. А. Грачева. – Текст : непосредственный // Вестник Российского университета кооперации. – 2022. – № 4 (50). – С. 93–100.

14. *Колычева А. Н.* Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : диссертация на соискание ученой степени кандидата

юридических наук / А. Н. Колычева. – Москва, 2018. – 199 с. – Текст : непосредственный.

15. Криминалистика : учебник / Б. Е. Богданов, А. Н. Васильев, В. Я. Колдин и др.; отв. ред. А. Н. Васильев. – М. : Изд-во Моск. ун-та, 1971. – 564 с. – Текст : непосредственный.

16. Криминалистика : учебник : в 5 томах. Том 3. Криминалистическая техника / под ред. И. В. Александрова. – М. : Юрайт, 2019. – 216 с. – Текст : непосредственный.

17. Мещеряков В. А. Теоретические основы механизма следообразования в цифровой криминалистике / В. А. Мещеряков. – Москва : ООО «Проспект», 2022. – 176 с. – Текст : непосредственный.

18. *Мочалов А. Н.* Об учреждении в России должности уполномоченного по защите прав человека в сфере информационно-телекоммуникационных технологий / А. Н. Мочалов. – Текст : непосредственный // Правовое государство: теория и практика. – 2022. – № 2 (68). – С. 27–39.

19. *Муленков Д. В.* Особенности назначения судебно-компьютерных экспертиз / Д. В. Муленков. – Текст : непосредственный // Криминалистика: вчера, сегодня, завтра. – 2015. – Выпуск 6. – С. 154–161.

20. *Нугаева Э. Д.* Особенности производства осмотра места происшествия по преступлениям, связанным с незаконным сбытом наркотических средств и психотропных веществ, совершенным дистанционным способом / Э. Д. Нугаева. – Текст : непосредственный // Экспертная практика. – 2023. – № 2 (94). – С. 36–47.

21. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, С. Р. Низаева, В. Р. Гайнельзянова, З. И. Харисова. − Уфа : Уфимский юридический институт МВД России, 2023. – 96 с. – Текст : непосредственный.

22. *Прокофьев А. А.* Участие специалиста при изъятии цифровых мобильных устройств / А. А. Прокофьев. – Текст : непосредственный // Актуальные проблемы криминалистики и судебной экспертизы : мат-лы междунар. науч.-практ. конф. Иркутск : Восточно-Сибирский институт МВД России, 2021. – С. 163–166.

23. Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров. – Москва : ЭКЦ МВД России, Следственный департамент МВД России, ГУНК МВД России, 2020. – С. 17 . – Текст : непосредственный.

24. *Россинская Е. Р.* Криминалистика : учебник для вузов. – М. : Норма-ИНФРА-М, 2016. – 464 с. – Текст : непосредственный.

25. *Россинская Е. Р.* Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе : монография / Е. Р. Россинская ; 4-е изд. – М., 2025. – 576 с. – Текст : непосредственный.

26. *Рудых А. А.* Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : диссертация на соискание ученой степени кандидата юридических наук / А. А. Рудых. – Ростов-на-Дону, 2020. – 239 с. – Текст : непосредственный.

27. *Саенко Г. В.* Компьютерная экспертиза / Г. В. Саенко, О. В. Тушканова. – Текст : непосредственный // Типовые экспертные методики исследования веще-

ственных доказательств. Ч. I / под ред. канд. техн. наук Ю. М. Дильдина ; общ. ред. канд. техн. наук В. В. Мартынова. – Москва : ЭКЦ МВД России, 2010. – 568 с.

28. Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков. – Москва : ООО «Проспект», 2023. – 256 с. – Текст : непосредственный.

29. Типовая методика исследования информации в мобильных телефонах / О. В. Тушканова [и др.]. – М., 2014. 32 с. – Текст : непосредственный.

30. *Третьякова Е. И.* Допрос несовершеннолетнего: процессуальные и тактические аспекты / Е. И. Третьякова. – Текст : непосредственный // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIV международной научно-практической конференции, Иркутск, 6–7 июня 2019 г. / Восточно-Сибирский институт МВД России. – Иркутск : Восточно-Сибирский институт МВД России, 2019. – С. 250–252.

31. *Третьякова Е. И.* Возможности деанонимизации лиц, совершающих мошенничество с применением спуффинг-атак / Е. И. Третьякова, С. С. Босхолов, Р. П. Щербина. – Текст : непосредственный // Криминалистика: вчера, сегодня, завтра. – 2021. – № 4 (20). – С. 106–118.

32. *Усачев С. И.* Особенности использования специальных знаний при расследовании мошенничества в сфере автострахования : диссертация на соискание ученой степени кандидата юридических наук / С. И. Усачев. – Калининград, 2022. – 222 с. – Текст : непосредственный.

33. *Цветков Н. А.* Тактика допроса подозреваемого и обвиняемого в конфликтной ситуации / Н. А. Цветков. – Текст : непосредственный // Вестник современных исследований. – 2018. – № 11 (26). – С. 334–339.

34. *Шевченко Е. С.* Тактика производства следственных действий при расследовании киберпреступлений : диссертация на соискание ученой степени кандидата юридических наук / Е. С. Шевченко. – Москва, 2016. – 249 с. – Текст : непосредственный.

Ресурсы информационно-телекоммуникационной сети Интернет

1. Кодификация.РФ. Действующее законодательство Российской Федерации. – URL: https://rulaws.ru.

2. Официальный портал судов общей юрисдикции города Москвы. – URL: https://mos-gorsud.ru.

3. Официальный сайт Известия. – URL: https://iz.ru.

4. Официальный сайт Министерства внутренних дел Российской Федерации. – URL: https://мвд.рф.

5. Справочная правовая система КонсультантПлюс : сайт. URL: https://www.consultant.ru/.

6. Судебные и нормативные акты РФ. – URL: https://sudact.ru.

7. Цифровой образовательный ресурс IPR SMART. – URL: https://www.iprbookshop.ru.

ПРИЛОЖЕНИЕ

Практические задания

ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 1

Неизвестное лицо уже несколько дней пытается нарушить работу форума на сайте администрации г. Иркутска, а также присылает письма с угрозами, что в ближайшее время взломает всю сеть администрации г. Иркутска. Единственная информация о неизвестном: он всегда подписывается ником «angryhackerirk777».

Задание:

Получите возможную информацию об этом пользователе.

Примерный план работы:

1. Проверить ник «angryhackerirk777» по поисковикам (google, яндекс).

2. Просмотреть имена в социальных сетях, при нахождении удаленных анкет воспользоваться «Веб-архивом».

3. Проверить, зарегистрированы ли почтовые адреса с таким ником (@mail.ru; @google.com и др.).

4. Проверить популярные форумы, где могут участвовать люди компьютерно-технической направленности (один из самых известных – «ГитХаб» https://github.com/).

5. При установлении таких пользователей направить запросы на эти площадки для получения информации о пользователе angryhackerirk777 (регистрационные данные, адреса электронной почты, номера сотовых телефонов при наличии двухфакторной аутентификации, даты выхода в сеть, IP-адреса, с которых осуществлялся выход на платформу).

ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 2

Гражданин Левин в информационно-телекоммуникационной сети Интернет приобрел компьютерную программу NNN, позволяющую без ведома владельцев мобильных телефонных аппаратов под управлением операционной системы «Android», являющихся держателями банковских карт ПАО «Сбербанк» с подключенной услугой «Мобильный банк», отправлять от их имени SMS-сообщения с командами о запросе баланса денежных средств, находящихся на счетах владельцев банковских карт, и о переводе денежных средств с данных счетов на счета третьих лиц без уведомления о произведенных операциях.

Затем Левин совместно с Федоровым от имени вымышленных лиц арендовали в ООО «1390», ЗАО «7585» и ООО «6451» веб-серверы, которым присвоили доменные имена W1, W2, W3 и на которых затем разместили компьютерную программу NNN. Левин также занимался тестированием компьютерной программы NNN, совершенствовал ее, устранял возникающие ошибки в веб-скриптах путем написания программного кода (PHP), который включал в себя добавление команд для проверки баланса на банковских картах ПАО «Сбербанк» и перевода денежных средств со счетов банковских карт граждан на подконтрольные Левину и Федорову номера мобильных телефонов или банковские счета, оформленные на лиц, не подозревающих о его и Федорова деятельности.

Через сеть Интернет Левин подыскивал номера сотовых телефонов граждан, являющихся держателями банковских карт ПАО «Сбербанк», и совместно с Федоровым занимался SMS-рассылкой сообщений, содержащих ложные сведения со ссылками на адреса веб-серверов, где была размещена компьютерная программа NNN. С целью конспирации своей деятельности от правоохранительных органов Левин использовал компьютерную программу «OpenVPN», предназначенную для сокрытия IP-адресов, с которых осуществлялись соединения с веб-серверами, где находилась компьютерная программа NNN, а также с электронными платежными системами, на счета которых ими перечислялись похищенные у граждан денежные средства.

После того, как обманутые граждане – держатели банковских карт ПАО «Сбербанк» с подключенной услугой «Мобильный банк» переходили по ссылкам на адреса W1, W2, W3 веб-серверов, где была размещена компьютерная программа NNN, что влекло за собой ее установку на сотовые телефоны данных граждан втайне от них, Левин и Федоров получали информацию о моделях мобильных телефонов, их серийных номерах (IMEI), о контактах пользователей телефонов, о подключенных к номерам мобильных телефонов граждан банковских картах и о наличии денежных средств на счетах этих карт.

Пользуясь тем, что компьютерная программа NNN блокировала входящие SMS-сообщения гражданам о списании их денежных средств со счетов банковских карт, от имени владельцев абонентских номеров мобильных телефонов Левин и Федоров отправляли SMS-сообщения на номер «900» автоматизированной системы обработки и хранения компьютерной информации, принадлежащий ПАО «Сбербанк», и осуществляли тем самым переводы денежных средств со счетов банковских карт граждан без их ведома на подконтрольные Левину и Федорову банковские счета и номера мобильных телефонов. Когда банк на основании их команд осуществлял такие переводы денежных средств, Левин и Федоров получали возможность распоряжаться похищенными у потерпевших

деньгами по своему усмотрению.

Задание.

Дайте правовую оценку деятельности Левина и Федорова.

Определите способ совершения преступления.

Что является местом совершения преступления?

Определите необходимость производства осмотра места происшествия. Что подлежит осмотру и отысканию?

Определите источники получения криминалистически значимой информации.

Какие экспертизы следует назначить? Какие задачи они будут решать? Что будет выступать в качестве объекта исследования?

Сформируйте перечень вопросов на соответствующую экспертизу при исследовании:

а) изъятого ноутбука Левина;

б) мобильного телефона потерпевшего.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 3

В ОП-1 г. Иркутска обратилась гр. Скворцова О. П. и пояснила: на сайте интернет-магазина ООО «Находка+» ею был оформлен заказ на покупку многофункционального лазерного устройства марки «Kyocera M2040DN (1102S33NL0) A4 Duplex белый/серый» за 28 546 рублей 98 копеек. В этот же день она оплатила заказ в полном объеме, сроки поставки – 25 рабочих дней, переписка с представителями интернет-магазина велась через электронную почту «naxodka+@mail.ru». На сайте данного интернет-магазина был указан номер телефона № 89055555555, на который она впоследствии неоднократно звонила, но никто не брал трубку телефона. Товар ей не поставлен, деньги не возвращены. Ущерб для нее значительный.

Задание.

Оцените ситуацию и дайте правовую оценку действиям неустановленного лица.

Какая информация, имеющая криминалистическое значение, не была выяснена при опросе?

Что может являться источником информации о преступнике?

Каким образом возможно получить эту информацию?

Проведите осмотр переписки гр. Скворцовой с продавцом. Какие сведения в ходе такого осмотра возможно получить? Какие процессуальные требования должны были соблюдены?

Определите комплекс первоначальных следственных действий и тактику их проведения.

Какие экспертизы можно назначить? Какие задачи они должны решить?

ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 4

Потерпевшая Иванова в ходе допроса на стадии предварительного расследования показала, что она решила заказать вещи для детей с помощью сети Интернет. Она через свой мобильный телефон зашла в приложение «Одноклассники», где у нее в друзьях был «Модный базар». Пройдя на страницу «Модный базар», она стала выбирать вещи для своих детей. Выбрав вещи, она отправила сообщение в «Одноклассниках» «Модный базар», после чего ей написали стоимость данных вещей. Ее данная стоимость устроила, после чего они в переписке оговорили оплату. Она должна была перевести по номеру карты № 4800000015232000 денежные средства в размере 10 000 рублей. Так как у Ивановой нет своей карты, она попросила свою подругу Бибикову перевести по данному номеру карты денежные средства в размере 10 000 рублей, на что Бибикова согласилась. После чего Иванова в банкомате на карту Бибиковой перевела денежные средства в сумме 10 000 рублей, а Бибикова затем перевела денежные средства в сумме 10 000 рублей на вышеуказанный номер карты. Комиссия составила 100 рублей. После Иванова пошла домой. Придя домой, она написала сообщение на странице «Модный базар», скинув чек об оплате, на что «Модный базар» прислал ей сообщение, что получили денежные средства, а также написали сообщение, что необходимо дождаться тега отслеживания посылки. Ивановой пришло сообщение от «Модный базар» с тегами отслеживания, которых было два, после чего она стала отслеживать через Интернет на сайте «Почта России» данные теги, но по ним посылки приходили в другие города. После этого она снова написала сообщение в «Модный базар», что у нее нет оповещения о доставке. Затем она получила другой тег, по которому также посылка была доставлена в другой город, после чего Иванова написала сообщение в «Модный базар», чтобы ей вернули денежные средства, на что ей ответили, что нужно открыть «спор» и что поставщик вернет деньги. От «Модный базар» ей пришло сообщение с просьбой написать ее номер карты, на которую ей смогут перечислить денежные средства. Иванова написала номер банковской карты, после чего ей пришло сообщение о том, что возврат будет через 10 дней. Через 10 дней деньги ей никто не вернул, и она обратилась в полицию.

Задание.

Оцените ситуацию и дайте правовую оценку действиям неустановленного лица.

Как, где и какую информацию можно получить о лице, на счет которого были переведены денежные средства?

Определите комплекс первоначальных следственных действий и тактику их проведения.

Каким образом можно просмотреть содержимое страницы интернет-

магазина «Модный базар» в случае, если в страницу были внесены изменения или она была удалена?

Как можно установить лиц, которые создали и администрировали страницу в Интернете?

Старичков Максим Владимирович,
кандидат юридических наук, доцент;
Третьякова Елена Игоревна,
кандидат юридических наук, доцент;
Усачев Сергей Игоревич,
кандидат юридических наук
(Восточно-Сибирский институт МВД России)

ТАКТИКА ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Руководитель проекта *М.Ю. Зимин*
Редактор *М.В. Мельников*
Компьютерная верстка *М.Д. Козина*

Подписано в печать 22.09.2025.
Формат $60\times90^{1}/_{16}$. Бумага офсетная.
Гарнитура Times New Roman.
Усл. печ. л. 8,0. Тираж 1450 экз. Заказ № 4187.

Отпечатано в ООО «Типография «Миттель Пресс».
Адрес: 127254, г. Москва, ул. Руставели, д.14, стр. 6, офис 7.
Тел./факс: +7 (495) 619-08-30, 647-01-89.
E-mail: mittelpress@mail.ru, www.mittelpress.ru.