МВД России
Санкт-Петербургский университет

А. Р. Акиев, К. И. Сотников

ТАКТИКА СЛЕДСТВЕННОГО ОСМОТРА И ИССЛЕДОВАНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ СРЕДСТВ ТЕЛЕКОММУНИКАЦИИ И ИНТЕРНЕТА

Учебно-практическое пособие

Санкт-Петербург
2023

План-график 2023, поз. 67

УДК 343.35
ББК 67.51
А39

Акиев А. Р., Сотников К. И.

А39 Тактика следственного осмотра и исследования цифровой информации средств телекоммуникации и интернета : учебно-практическое пособие / А. Р. Акиев, К. И. Сотников. — Санкт-Петербург: СПбУ МВД России, 2023. — 68 с.

Авторский коллектив:
Акиев А. Р. (гл. 1, гл. 3 § 3.1);
Сотников К. И. (введен., гл. 2, гл. 3 § 3.2, закл.)

ISBN 978-5-91837-716-1
EDN LBAHYP

В современных условиях широкого использования информационных технологий, интеллектуализации преступности, в связи с усложнением механизма совершения преступлений, изменениями уголовного и уголовно-процессуального законодательства работа с электронной информацией как со сложной системой сведений об обстоятельствах преступления требует особого подхода и определенного уровня криминалистических знаний в области цифровых технологий. Особую значимость такая информация приобретает по делам о готовящихся или совершенных преступлениях против личности, в сфере экономической деятельности, мошенничестве, незаконном обороте наркотических средств, экстремизме и терроризме. Особенности создания, хранения, уничтожения и пересылки электронной информации обусловили проблему тактики ее обнаружения в виртуальных сетях и на компьютерных устройствах, процессуальной фиксации и использования таких сведений в ходе раскрытия и расследования преступлений.

Предлагаемое учебно-практическое пособие может быть использовано в учебном процессе в рамках изучения учебной дисциплины «Криминалистика», на курсах повышения квалификации дознавателей и следователей ОВД. Пособие представляет интерес для научно-педагогических и практических работников системы органов МВД России.

Предназначено для обучающихся в образовательных организациях высшего образования системы МВД России по специальностям (направлению подготовки): 40.05.01 — правовое обеспечение национальной безопасности; 40.05.02 — правоохранительная деятельность; 40.03.01 — юриспруденция.

УДК 343.35
ББК 67.51

Рецензенты:
Макарова Н. Ю., кандидат юридических наук
(СУ УМВД России по Приморскому району г. Санкт-Петербурга)
Рясов А. А., кандидат юридических наук, доцент
(Ставропольский филиал Краснодарского университета МВД России)

ISBN 978-5-91837-716-1

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современных условиях широкого использования средств телекоммуникации и интернета работа с электронной информацией как со сложной системой сведений об обстоятельствах преступления требует особого подхода и определенного уровня криминалистических знаний в области цифровых технологий.

В настоящее время компьютерные технологии активно внедряются в деятельность правоохранительных органов, в уголовное судопроизводство, криминалистику и в экспертную практику. Цифровые технологии находят применение в электронном документообороте, накоплении и обработке криминалистической значимой информации, использовании программных продуктов при проведении судебных экспертиз и т. п. Внедрение цифровых технологий в практику раскрытия и расследования преступлений способствует повышению эффективности работы правоохранительных органов, ускоряет процесс накопления и переработки информации, облегчает подготовку, формирование, обработку передачу процессуальных и иных документов, автоматизирует производство экспертных исследований.

В юридическую науку, и криминалистику в том числе, входят такие понятия, как «цифровые технологии», «право и цифровизация», «цифровизация правосудия», «цифровая среда в уголовном процессе», «электронный документ», «электронное делопроизводство», «электронное уголовное дело». Разработаны научные основы и формируется современная практика обнаружения, исследования и использования цифровых следов в целях раскрытия и расследования преступлений. Глубоко исследованы тактика фиксации, изъятия цифровых следов на электронных носителях и в сети «Интернет», особенности назначения и проведения компьютерно-технических экспертиз, а также методика расследования компьютерных преступлений.

Компьютерные устройства, средства телекоммуникации и сеть «Интернет» широко используются для совершения различных видов преступлений. Введен в оборот термин «киберпреступность», под которым понимается широкий круг преступных посягательств, связанных с цифровыми технологиями. При расследовании преступлений возникает потребность в изучении специфических цифровых источников доказательств, свидетельствующих о механизме и следовой картине совершения противоправного деяния. Важными источниками доказательств становятся цифровые (элек-

тронные) носители криминалистической значимой информации: мобильные телефоны, смартфоны, компьютеры, ноутбуки, планшеты, компьютеры, GPS-навигаторы, внешние накопители электронной информации, сетевые устройства и интернет-ресурсы.

Особую значимость такая информация приобретает по делам о готовящихся или совершенных преступлениях против личности, в сфере экономической деятельности, мошенничестве, незаконном обороте наркотических средств, экстремизме и терроризме. В связи с особенностями создания, хранения, уничтожения и пересылки электронной информации существует проблема тактики ее обнаружения в виртуальных сетях и на компьютерных устройствах, процессуальной фиксации и использования таких сведений в ходе раскрытия и расследования преступлений.

С позиции тактики изъятия носителей электронной информации, осмотра их содержимого и интернет-сайтов, складывающейся практики и требований УПК РФ, сохраняется проблема поиска, фиксации, изъятия и сохранности электронной информации, связанной с совершением и сокрытием преступлений. В настоящем учебно-практическом пособии с учетом современного законодательства, складывающей правоприменительной практики и достижений науки криминалистики рассмотрены понятие и правовые основы функционирования телекоммуникационных сетей и современных ресурсов интернета. Проанализированы основные способы, механизм совершения преступлений с использованием телекоммуникационных сетей и интернета, виды электронных следов, тактика изъятия средств телекоммуникации и интернета, осмотра, фиксации, предварительного исследования и анализа электронной криминалистической информации. Перечислены виды, тактика назначения и особенности проведения судебных компьютерно-технических экспертиз по исследованию средств телекоммуникации и интернета.

ГЛАВА I
ПОНЯТИЕ И ПРАВОВЫЕ ОСНОВЫ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И ИНТЕРНЕТА

1.1. Понятие телекоммуникационных сетей и современных ресурсов интернета

Современный этап глобализации мира неразрывно связан с развитием процессов информатизации общества. Информационно-коммуникационные технологии затрагивают все социальные и экономические отношения в современном обществе. Под влиянием этих технологий образуется информационная инфраструктура, обеспечивающая функционирование и развитие информационного пространства и средств информационного взаимодействия в обществе. Развитие региональных информационных систем, их интеграция с международными информационными ресурсами, спутниковых систем и мобильной связи привели к созданию глобальной информационной телекоммуникационной инфраструктуры.

В соответствии со ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ***информационно-телекоммуникационная сеть (далее — ИТКС)*** — это техническая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Телекоммуникационными сетями являются: телефонные сети для передачи телефонных данных (голоса); радиосети для передачи аудиоданных; телевизионные сети для передачи видеоданных; цифровые (компьютерные) сети или сети передачи данных для передачи цифровых (компьютерных) данных. Телекоммуникационные сети представляют собой комплекс аппаратных и программных средств, обеспечивающих передачу информационных сообщений между абонентами с заданными параметрами качества.

Как подчеркнуто в постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет„», к числу компьютерных устройств могут

быть отнесены любые электронные устройства, 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 и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом.

В указанном постановлении под ***компьютерной информацией*** понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах (далее — компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе жестких дисках-накопителях, флеш-картах и т. п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи.

Телекоммуникация — это система технических электронных устройств, компьютерных технологий и программ, позволяющих передавать информацию по кабельным, радиотехническим и спутниковым каналам. Телекоммуникация представляет собой процесс получения и обработки информации с применением электронных, сетевых, информационных и компьютерных технологий. Современная телефонная связь с технической позиции является сотовой связью, соединяет в одну сеть мобильные устройства и позволяет переходить с аналогового на цифровой стандарты. Сеть «Интернет» представляет собой наиболее распространенный вид телекоммуникационных технологий. Телекоммуникация предполагает передачу всех форм информации между компьютерами посредством различных видов линий связи. Для обеспечения доступного обмена информационными файлами необходим доступ к сети «Интернет», соответствующее программное обеспечение для обработки данных и техническое средство (компьютер, планшет, смартфон).

Компьютерное устройство — это электронное оборудование, выполняющее информационные операции в цифровом формате и выдающее результаты в форме, воспринимаемой человеком или

машиной. Компьютерное оборудование включает в себя технические части компьютера: центральный процессор, видеокарту, звуковую карту, хранилище данных, материнскую плату, монитор, клавиатуру и др. Программное обеспечение — это набор инструкций, система электронных приложений, которые хранятся и выполняются аппаратным обеспечением.

Особое место в системе телекоммуникации занимают ***смартфоны*** (англ. *smart phone* — умный телефон) — мобильный телефон с сенсорным экраном, который представляет собой миниатюрный универсальный компьютер с полноценным пользовательским интерфейсом мобильного телефона и монитора компьютера.

Компьютерная информация, содержащаяся на электронном носителе компьютера или смартфона, называется ***файлом***. Каждый файл имеет свои атрибуты, позволяющие его идентифицировать: индивидуальные цифровые выходные данные, название, тип файла (текстовый или графический), его назначение, объем представленной информации и др. Компьютеры делятся на стационарные, портативные, малогабаритные, могут иметь периферийные устройства различного назначения, а также сервера (мощные компьютеры для выполнения какой-либо сервисной задачи без участия человека), предназначаться для индивидуальных пользователей, системных операторов и т. д. Компьютер в сочетании с периферийными устройствами образует компьютерную систему. К периферийным устройствам относят мышь, графический планшет, сенсорный экран, микрофон, сканер, веб-камеру, клавиатуру, акустическую систему, принтер, монитор, накопители на магнитных дисках, USB-флеш-накопитель и др.

Мобильный интернет — это технология подключения с помощью мобильного устройства (телефона, смартфона) к сети «Интернет» из любого местонахождения пользователя. Мобильная связь служит для передачи и получения данных от одного абонента другому пользователю мобильным телефоном или компьютерным устройством. Развитие современных технологий обеспечивает мобильный доступ к ресурсам интернета. Технические службы мобильной передачи данных предоставляют абонентам широкий выбор онлайновых услуг: совершение банковских операций, покупку товаров, проведение различных платежей, обмен информационными файлами, поиск объектов и услуг. Возможности телекоммуникации в сети «Интернет» зависят от технического устройства, программного обеспечения и имеющегося объема электронной памяти.

Интернет-ресурс (синонимы «веб-ресурс, веб-сайт, веб-сервис, сайт) характеризуется интегрированной системой средств технического и программного обеспечения, зависит от объема информации, размещенной во Всемирной паутине. В широком понимании интернет-ресурс представляет собой совокупность электронных документов или файлов, объединенных одним IP-адресом или доменом. Все интернет-ресурсы расположены на удаленных друг от друга работающих серверах, совокупность которых называется Всемирной паутиной. Именно она объединяет между собой различные фрагменты информации сети в единое целое.

Интернет-ресурс содержит информацию в текстовой, графической и мультимедийной форме. Каждый интернет-ресурс имеет уникальный IP-адрес, который позволяет выделить и идентифицировать его в Сети.

Интернет-сайты делятся на свободные (доступные), когда любой пользователь может попасть на данный ресурс, либо закрытые, посещение которых требует регистрации и специального порядка доступа. Существуют так называемые ***интернет-порталы***, объединенные по целевому назначению, обладающие сложной иерархией, состоящие из множества страниц и включающие значительный объем информации. Портал может состоять из множества взаимозависимых сайтов, посвященных определенной тематике и поставленных специальных задач.

Отдельного внимания заслуживают интернет-представительства и веб-сервисы. Интернет-представительства дают информацию пользователям о каком-либо бизнесе, компании, проекте и т. д. Веб-сервисы созданы для выполнения определенных технических задач сети «Интернет» (хостинги, поисковики, доски объявлений, почтовые сервисы, форумы и т. п.).

Важное место в числе интернет-ресурсов отводится ***сайтам или веб-сайтам*** (от англ. *website*: *web* — паутина, сеть и *site* — место), которые включают в себя объединенные общей структурой документы со ссылками (веб-страницы). Страницы сайтов — это набор текстовых файлов, которые, будучи загруженными пользователем на компьютер, обрабатываются ***браузером*** и выводятся на монитор либо на экран смартфона, принтер или синтезатор речи. ***Веб-узел*** **—** одна или несколько логически связанных между собой веб-страниц и место расположения контента-сервера. ***Контент*** **—** содержимое сайта (тексты, картинки, графика, музыка, видео и др.). Текстовое содержа-

ние позволяет пользователям найти соответствующих сайт с использованием поисковых систем.

Поисковая система — это программы и сайты, выдающие по запросу пользователя соответствующую информацию и документы. Популярными поисковикам являются Yandex, Google и др. В основе поиска нужной страницы лежит доменное имя (адрес), по которому его можно найти в интернете. Доменное имя представляет собой набор англоязычных или русских символов, которые пользователь вводит в адресную строку браузера. Часто в качестве домена используют название компании либо фамилию владельца, входящего на страницы интернет-сайтов.

По целям и выполняемым задачам сайты представляется условно классифицировать по различному назначению:

— персональные (домашние) страницы пользователей с личной информацией;

— сайты-визитки — дают общую информацию об организации или предприятии, используются для контакта с возможными посетителями; на такие сайты заходят, чтобы узнать адрес организации, посмотреть местоположение или каталог, прайс-лист товаров;

— информационные сайты — одни из самых распространенных в интернете типов сайтов. Они содержат информацию, включающую в себя различные тематические разделы о порядке взаимодействия с пользователями и позволяют пользователям общаться в рамках портала (форумы, чаты). Для информационных сайтов характерна доступность информации. Информационные порталы содержат рекламную информацию в текстовом, графическом или каком-либо другом виде. Посетители могут скачивать документы, картинки, фотографии, видеофильмы и т. п.;

— промо-сайты — посвященные разовым событиям или акциям; используются для рекламы товаров, продуктов, могут содержать галерею с акциями распродаж товаров;

— сайты-фотогалереи — позволяют загружать личные фотографии, рисунки, картины; пользователи могут поделиться своими изображениями в сети или просто хранить фотоальбомы в облачном хранилище на серверах.

— информационные интернет-издания, средства массовой информации — информируют о последних событиях в реальном времени, работают параллельно с телевизионными каналами новостей, печатными изданиями, регулярно обновляются свежей информацией;

— сайты интернет-магазинов — предназначены для продажи различных товаров и услуг. Такие сайты представляет собой каталог товаров с подробным описанием, фотографии, имеются отзывы покупателей. Покупку можно оплатить в режиме онлайн при получении товара, а также выбрать вариант доставки. В последнее время интернет-магазины получили большое распространение;

— сайты-сервисы позволяют пользователям обрабатывать информацию, рисунки и фотографии, переводить тексты, сравнивать различные сайты и т. д. Существуют крупные порталы (Яндекс, Google), предоставляющие множество различных услуг;

— сайты социальных сетей (Одноклассники, Вконтакте, Twitter, Facebook), которые имеют своей целью создание условия для виртуального общения людей, обмена между ними информацией.

Высока популярность так называемых блогов, появилось новое понятие — блогосфера. В отличие от иных сайтов, блоги предоставляют в сети информацию по интересующей пользователя тематике. Они бывают личные или корпоративные, тематические, посвященные какой-то конкретной теме. Каждая статья в блоге называется постом, который публикуется от имени автора, обозначается дата публикации. На подобную информацию посетители реагируют репостами, переносят на свой компьютер, размещают в социальных сетях, комментируют.

Следует отметить, что деление сайтов носит условный характер. Многие сайты сочетают в себе различное содержание и предназначение других сайтов. Существует множество сайтов, на которых могут располагаться персональные данные пользователей (адреса, телефоны, личная переписка). Так, на сайтах банковских учреждений помещается информация о предоставляемых услугах банка. При взломе этих ресурсов похититель может перечислить деньги с чужого счета на собственный счет, завладеть конфиденциальной информацией, изменить содержимое сайта. В целях исключения взлома сайтов программистами и соответствующими службами организации создается система электронной безопасности.

Широкое распространение получили сайты о предоставлении различных услуг и сервисы объявлений: «Яндекс.услуги», «Авито», «Юла», «Из рук в руки», «Купи Продай», «Маркет Вконтакте», «Профи.Ру» и др.

Новые технологии предоставляют возможность оперативного обмена, обработки, передачи и анализа информации, размещаемой в сети «Интернет». Открытость технологий и возможность создания

web-сайтов с любым содержанием создает угрозу для достоверности и надежности информации, использовании ее в преступных целях и причинении различного вреда пользователям (материального, репутационного), а также посягать на основы общественной и государственной безопасности.

Особое место в числе интернет-ресурсов занимают ***мессенджеры*** (от англ. *messenger* — курьер) — специальные приложения, которые устанавливают на смартфон или компьютер. Основная цель мессенджера — мгновенный обмен с другими пользователями текстовыми сообщениями, файлами документов, голосовыми сообщениями, фотографиями, картинками, видеороликами. Мессенджеры в режиме онлайн выступают в виде электронной почты быстрого обмена информацией. С их помощью можно совершать телефонные звонки, использовать аудио- или видеосвязь. Сообщения отправляются собеседнику после того, как отправитель закончит ввод, редактирование текста. Обмен сообщениями идет в режиме реального времени. Кроме того, мессенджер позволяет создавать группы пользователей (чаты) для общения в группе по интересам на работе, учебе, в формальных группах, а также проводить дистанционное обучение по различной тематике. Большинство мессенджеров предлагают функцию хранения переписки в облачных хранилищах. Мессенджер выполняет контактную, информационную, побудительную, координационную, мотивационную, воздействующую функции. Посредством общения через мессенджеры можно направлять участников общения на выполнение определенных действий, влиять на их поведение, согласовывать их действия, изменять намерения и мнения относительно какого-либо общественно значимого события.

К наиболее популярным зарубежным мессенджерам относятся: WhatsApp, Viber, Facebook Messenger, Telegram, Skype, Hangouts Google, Signal и др. Самой популярной программой в настоящее время считается WhatsApp. Довольно развиты отечественные мессенджеры: Mail.ru, Агент, МТС Коннект, TamTam, Яндекс.

Подобными сервисами активно пользуются наркоторговцы для бесконтактной реализации наркотиков, экстремисты, террористы, побуждающие к совершению определенных действий. Использование телекоммуникационных сетей и современных ресурсов, интернета осложняет работу правоохранительных служб и силовых ведомств по обеспечению общественной и государственной безопасности.

При этом использование современных информационных технологий позволяет эффективно и оперативно противодействовать совершению наиболее опасных преступлений, своевременно получать объективную информацию о подготовке, совершении и сокрытии преступлений, поэтому перед следователями, дознавателями и оперативно-розыскными подразделениями стоит задача поиска, сохранения, изъятия и исследования электронных (виртуальных) следов в сети «Интернет», их процессуального закрепления в целях раскрытия и расследования преступлений.

1.2. Правовое регулирование функционирования телекоммуникационных сетей и интернета в России

Правовые отношения в сфере функционирования телекоммуникационных сетей и интернета в Российской Федерации регулируются большим пакетом нормативных правовых актов. Основным нормативным документом, юридически описывающим понятия и определения в области информационных технологий, правового регулирования этой сферы является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данный закон определяет следующие основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при несанкционированных атаках на ее компьютерные сети и порталы. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» ориентирован на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Существенные изменения в порядке регулирования деятельности телекоммуникационных сетей и интернета в России внесены федеральными законами от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» и от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

Согласно этим законодательным актам и постановлениям правительства, интернет-компании должны хранить на своих серверах и предоставлять спецслужбам полные данные о личности пользователей, адреса электронной почты, хранить записи телефонных разговоров, тексты SMS-сообщений, аудио- и видеозаписи. В числе нововведений содержится требование о повышении срока хранения операторами мобильной связи информации о фактах приема, передачи и содержимого голосовой информации и сообщений от полугода до трёх лет.

В современной научной литературе употребляются термины «киберпреступность», «киберпреступления». Применительно к отдельным видам преступлений используются термины «кибертерроризм», «киберторговля наркотиками», «киберпорнография». В Конвенции ООН «О киберпреступности» от 1 июля 2004 г. к киберпреступлениям относятся деяния, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей

и компьютерных данных, злоупотребления такими системами, сетями и данными. По рекомендации экспертов ООН к киберпреступлениям следует относить все преступления, в которых компьютер, информационно-телекоммуникационные технологии или сети выступают предметом, средством или орудием преступления. Данная группа преступлений включает в себя как информационные компьютерные преступления и любые иные преступления, которые так или иначе связаны с применением компьютеров, информационно-телекоммуникационных технологий или сетей.

В отечественной юридической литературе под ***киберпреступлениями*** понимают преступления в сфере компьютерной информации, информационные преступления, а также преступления, связанные с компьютерными техническими средствами, преступления в сфере высоких компьютерных технологий и в информационном пространстве.

В широком смысле слова компьютерная преступность представляет собой совокупность преступлений, основным объектом которых выступают общественные отношения в сфере компьютерной информации и информационных технологий, защиты компьютерной информации, безопасного функционирования технических средств (компьютеры, планшеты, ноутбуки, смартфоны, банкоматы, платежные терминалы и др.).

В узком смысле слова компьютерная преступность представляет собой совокупность предусмотренных законодательством преступлений, в которых предусмотрена уголовная ответственность за посягательства на безопасность компьютерной информации, функционирование информационно-телекоммуникационных сетей, а также средства хранения, обработки и передачи компьютерной информации.

В Уголовном кодексе РФ отсутствует определение киберпреступления. Законодателем определена глава 28 УК РФ «Преступления в сфере компьютерной информации». Можно выделить три группы преступлений, связанных с использованием телекоммуникационных сетей и интернета.

К *первой группе* следует отнести преступления, предусмотренные главой 28 УК РФ «Преступления в сфере компьютерной информации»: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на крити-

ческую информационную инфраструктуру Российской Федерации (ст. ст. 272–274[1] УК РФ).

Ко *второй группе* преступлений относятся деяния, в которых использование информационных технологий включено в качестве элемента состава преступления или отягчающего обстоятельства, повышающего ответственность за совершение указанного преступления. Так, в 2012 г. в УК РФ были введены статьи, регламентирующие уголовную ответственность за различные виды кибермошенничества: ст. 159[3] «Мошенничество с использованием электронных средств платежа» и ст. 159[6] «Мошенничество в сфере компьютерной информации.

Повышенная уголовная ответственность установлена за совершение с использованием телекоммуникационных сетей и интернета следующих преступлений: ст. 110 «Доведение до самоубийства»; ст. 128[1] «Клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации либо совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть "Интернет"»; ст. 242 «Незаконные изготовление и оборот порнографических материалов»; ст. 242[1] «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»; ст. 151[2] «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего»; ст. 205[2] «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма»; ст. 280 «Публичные призывы к осуществлению экстремистской деятельности»; ст. 280[1] «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации» и ст. 354[1] «Реабилитация нацизма».

Кроме того, в новой ст. 284[2] УК РФ устанавливается ответственность за призывы к введению мер ограничительного характера в отношении Российской Федерации, граждан РФ или российских юридических лиц, совершенные гражданином РФ после его привлечения к административной ответственности за аналогичное деяние в течение одного года. В качестве отягчающего обстоятельства выступает использование средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет».

В УК РФ включена ст. 207[3], устанавливающая ответственность за публичное распространение под видом достоверных сообщений заведомо ложной информации об использовании Вооруженных Сил РФ

в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, а также ст. 280^3, предусматривающая ответственность за публичные действия, направленные на дискредитацию использования Вооруженных Сил РФ, в том числе за публичные призывы к воспрепятствованию их использования в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, совершенные лицом после его привлечения к административной ответственности за аналогичное деяние в течение одного года. В указанных статьях нет ссылок на использование телекоммуникационных сетей и интернета, вместе с тем, как показывает судебная практика, эти виды преступлений, как правило, совершаются с использованием телекоммуникационных сетей и интернета.

Отдельно следует назвать ст. 187 УК РФ, предусматривающую ответственность за неправомерный оборот средств платежей, предполагающий изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты (за исключением случаев, предусмотренных ст. 186 УК РФ), а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств.

К *третьей группе* следует отнести преступления, для совершения которых современные средства телекоммуникации используются исключительно как средство связи и передачи информации на стадиях подготовки, совершения и сокрытия преступлений. По сути, к указанной группе, при наличии этого обстоятельства, может быть отнесено любое преступление (кража, убийство, изнасилование, взяточничество и др.). Использование средства телекоммуникации и интернета облегчает совершение преступления, однако следователи и сотрудники оперативных служб получают дополнительные доказательства, способствующие раскрытию и расследованию события преступления.

1.3. Типичные способы и следы совершения преступлений с использованием телекоммуникационных сетей и интернета

Для киберпреступлений характерна трансграничность, межрегиональность, интерсубъектность, т. е. возможность их совершения

из любой точки планеты, взаимодействие международных преступных сообществ и отдельных незнакомых лиц. Можно отметить нестандартность и множественность способов их совершения. Для киберпреступлений свойственна автоматизация действий, использование специальных познаний, а также высокий уровень анонимности и латентности деяний. Киберпреступность приносит высокие доходы (наркоторговля, мошенничество). Эти факторы обусловливают сложность раскрытия данного вида преступлений.

Преступления в сфере информационных технологий включают распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, распространение противоправной информации (клеветы, порнографии, материалов, возбуждающих межнациональную и межрелигиозную вражду и т. п.). Эти преступления связаны с использованием компьютерной техники, сетей интернета, программных продуктов, средств мобильной связи, банковских карт, фиктивных электронных платежей и др.

Наибольшую опасность представляют преступления, посягающие на общественную, государственную и личную безопасность, том числе в сфере экономики, государственного управления, имущественных отношений юридических и физических лиц.

В связи с изложенным предполагается рассмотреть лишь наиболее распространенные виды преступлений, типичные способы их совершения и следы, оставляемые при использовании телекоммуникационных средств и интернета.

В последние годы отмечается резкий рост мошенничества, совершенного с использованием телекоммуникационных сетей и интернета. Одним из самых распространенных способов интернет-мошенничества является так называемый ***фишинг*** (от англ. *phishing* — рыбалка), в ходе которого мошенник путем рассылки электронных писем пытается получить конфиденциальную информацию о пользователе, пароли, номера банковских карт. Мошенники создают видимость, что эти сообщения исходят от вызывающих доверие источников: торговой компании, банка, государственного учреждения и т. п. Посредством почтовых рассылок от имени банка, содержащих в себе ссылки на страницы копий официальных сайтов, предлагается ввести данные карты для возможности дальнейшего ее использования в целях похищения денежных средств пользователя.

Распространенным видом интернет-мошенничества являются *фальшивые интернет-магазины*, когда мошенники создают свои сай-

ты с использованием интернет-маркетинга. Платежные страницы на таких сайтах создаются под оплату товаров и услуг, а потенциальная жертва переводит деньги на карты мошенников или на номера их мобильных телефонов, с которых впоследствии будут сняты и похищены деньги. Кроме того, на поддельных сайтах мошенники собирают реквизиты карт, которые потом используют для несанкционированных операций.

Часто мошенники выдают себя за сотрудников банка. Под предлогом «сбоя в базе данных», «начисления бонусов», «подключения к социальной программе» или иных надуманных предлогов, мошенники просят сообщить им реквизиты карты, код безопасности и одноразовый пароль, приходящий на мобильный телефон или компьютер. Получив необходимые сведения, мошенники списывают деньги со счета жертвы.

Мошенничество под видом *благотворительности.* Мошенник представляется сотрудником благотворительной организации, собирающей средства на помощь жертвам стихийного бедствия, террористической атаки, регионального конфликта или эпидемии, больным детям и т. п.

Мошенничество с *билетами* на зрелищные мероприятия является одной из разновидностей мошенничества в интернет-маркетинге. Распространение онлайн-агентств по продаже билетов способствует этому виду мошенничества. Мошенники продают фальшивые билеты на популярные мероприятия (концерты, шоу, спортивные игры) и присваивают деньги пользователя.

В последнее время преступники используют подарочные карты магазинов. Хакеры похищают данные подарочной карты и используют имеющиеся на карте средства для покупки товаров или их перепродажи на стороннем интернет-сайте.

Телефонное мошенничество. В последние годы этот способ хищения получил сравнительно широкий размах. Зарегистрированы случаи телефонного мошенничества, совершаемого осужденными из мест лишения свободы. Телефонные мошенники звонят на мобильные телефоны граждан. Часто путем перебора номеров телефона звонят абоненту, который им не знаком, затем посредством постановки определенных вопросов диагностируют личность предполагаемой жертвы (возраст, семейное положение, наличие родственников, их местоположение и т. п.) и сообщают о проблемной ситуации, в которую попал его близкий родственник, предлагая решить ее за опреде-

ленную сумме денег (например, задержан за незаконный оборот наркотических средств, совершил дорожно-транспортное преступление). Такие звонки также могут поступать к абонентам, о которых мошенник располагает некоей информацией, полученной в ходе контактов с другими лицами либо в социальных сетях интернета.

Чаще всего такие звонки совершают с номеров, по которым не представляется возможным установить личность телефонного мошенника. Если телефонный номер зарегистрирован на подставное лицо, то для установления личности реального обладателя можно использовать сведения об оплате расходов за оказанные услуги связи. Необходимо установить подставное лицо, а через него реального пользователя искомым номером телефона.

На первоначальном этапе расследования хищений, совершенных с использованием средств мобильной связи посредством телефонных звонков, можно установить абонентский номер, с которого поступил исходящий телефонный вызов либо SMS-сообщение, что позволяет выявить лицо, звонившее потерпевшему либо лицо, которому принадлежит конкретная SIM-карта. Указанная информация может быть получена в ходе допроса потерпевшего, следственного осмотра его мобильного устройства либо из представленной потерпевшим детализации его соединений в день совершения преступления.

Особую опасность в настоящее время представляют преступления, связанные с незаконным оборотом наркотических средств, совершенные с использованием информационно-телекоммуникационной сети и интернета. Применение мобильных телефонов и возможностей интернета позволило наркоторговцам модернизировать схемы поиска и контакта с потенциальными потребителями наркотических средств. Речь идет о дистанционной торговле наркотиками, позволяющей наркодельцам существенно расширить географию торговли, минимизировать риски, связанные с преступной деятельностью. Получили распространение онлайн-магазины на платформе интернет-торговли типа «Маркетплейс», которые представляют информацию о различных товарах и услугах. Реализация наркотических средств и психотропных веществ происходит посредством использования маркет-площадок, на которых представлен ассортимент товара, способы и меры безопасности приобретения, указаны ссылки, на другие мессенджеры. Широко используются для проведения сделки так называемые боты, способные без участия человека предоставить информацию о товаре, провести сделку и отправить координаты тайника наркотиков (закладок). Пере-

даются текстовые и иные сообщения о местах нахождения закладок наркотических средств, их фотографии с адресной привязкой к стационарным объектам (улица, номер дома или иного инфраструктурного объекта) для облегчения их поиска, а также используются системы навигации и определения координат нахождения тайников.

Могут быть даны наборы домофонных замков для проникновения «закладчиков» в подъезды многоквартирных домов. Имеются инструкции и наставления об организации своего наркобизнеса, об особенностях работы «закладчиком», «кладовщиком», «курьером». Представлены инструкции и видеоуроки по производству наркотических средств и психотропных веществ, продаются прекурсоры, химические вещества, лабораторное оборудование для синтеза наркотических средств и психотропных веществ. Для обхода государственных средств электронной защиты используются различные программы, позволяющие анонимно осуществлять противоправные сделки и преступные действия.

Владельцы и администраторы указанных торговых площадок предоставляют возможность продавцам и производителям размещать свои предложения о продаже наркотических средств, не имея непосредственного отношения к незаконному обороту наркотиков. В платформу интегрирована система шифрования сообщений между пользователями (продавцы, покупатели, администрация) и система конвертации виртуальных денег (криптовалют). Преступниками используется программное обеспечение, позволяющее изменять IP-адрес абонентского устройства, так называемые VPN-сервисы, что исключает возможность поиска устройства по геолокации, дает возможность обхода блокировок интернет-ресурсов со стороны государственных органов. Расчеты производятся посредством электронных платежей с использованием криптовалюты, так называемых электронных кошельков (WebMoney, Яндекс.Money, Qiwi, PayPal, 5 ePayments) и др.

Можно заключить, что совершение электронного мошенничества, незаконного оборота наркотических средств и другие преступления с использованием ИТКС оставляют значительный объем так называемых виртуальных следов. Задача следователя, оперативных сотрудников и специалистов состоит в установлении способа совершения преступления, его механизма, своевременного обнаружения и анализа виртуальных следов, фиксации их на электронных и бумажных носителях, процессуального оформления факта изъятия и последующего исследования в рамках судебных экспертиз.

Под виртуальными (электронно-цифровыми, компьютерными) следами понимается любая криминалистически значимая компьютерная информация, находящаяся в электронно-цифровой форме, зафиксированная на материальном носителе либо передающиеся по каналам связи через ИТКС и интернета. Виртуальные следы содержат сведения о совершении любых действий (входе, создании, внесении изменений, удалении информации) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей. Компьютерные следы представляют собой особую форму материальных следов-отображений, зафиксированных на электронных цифровых носителях, которые возможно объективизировать на мониторе, распечатать на бумажный носитель, произвести копирование на иной электронный носитель информации.

Различают локальные и сетевые компьютерные следы. ***Локальные следы*** могут храниться в смартфонах, компьютерах и иных носителях электронной информации. ***Сетевые следы*** располагаются на серверах, в облачных хранилищах и в ином коммуникационном оборудовании. Сетевые следы представляют собой сведения о сообщениях по сетям электронной связи либо сохраняемых поставщиками услуг (провайдерами) о состоявшихся сеансах связи или переданных сообщениях.

Сведения о пользователе компьютером, в том числе смартфоном, включают: имя, адрес, дату рождения, номер телефона, IP-адрес пользователя, данные о поставщике услуг интернета (провайдере), адрес электронной почты, идентификационные данные банковского счета при осуществлении платежных операций за услуги, перечень предоставляемых услуг и др. Сведения о сообщениях содержат дату и время сеанса связи, иную информацию. Электронная информация может храниться в виде текстовых, графических, видеофайлов, переноситься с одного электронного носителя на другой, воспроизводиться с помощью браузера.

Местом обнаружения виртуальные следов могут быть ресурсы интернета, профиль пользователя в социальных сетях, базы данных операторов связи, государственных структур, банковской системы, электронные платежные системы, торговых площадок, социальные сети, мессенджеры и др., а также жесткие диски, карты памяти, персональные компьютеры, средства мобильной связи.

Значительный объем информации сведения сохраняется у поставщика интернет-услуг (провайдера). У операторов сотовой связи

можно получить детализацию входящих и исходящих звонков, текстовых и голосовых сообщений, SMS-сообщений банка о движении денежных средств, а также о получателе денег. Кроме того, у оператора могут быть получены данные о геолокации, сведения о фактах замены SIM-карты, журналы использования IP-адресов. Операторы платежных систем могут предоставить установочные данные пользователя, сведения о переводах, движении средств, сведения о получателях платежа, адреса электронной почты, абонентские номера и т. д. Путем изучения компьютера (смартфона) можно получить идентификационные данные используемого компьютерного оборудования (IMEI), сведения о «привязанных» к абонентскому номеру адресах электронной почты, персональных учетных данных в социальных сетях.

Важное значение имеет информация, хранящаяся на компьютере потерпевшего, которая может содержать переписку с мошенником, в том числе в социальных сетях, а также сведения о движении электронных денежных средств в платежных системах банков. Изучение компьютерной техники позволяет выявить вредоносные компьютерные программы, фишинговые сайты при попытках мошенников получить конфиденциальную информацию пользователей (данные банковской карты, ее логин, пароль, pin-код).

В кредитной организации (банке) можно установить паспортных данные лица, открывшего расчетный счет и получившего платежную карту, сведения о проведенных денежных операциях, местах их совершения, абонентских номерах мобильной связи по электронным кошелькам, электронным платежным терминалам и банкоматам.

В случае изъятия персонального компьютера, средств мобильной связи необходимо назначить компьютерно-техническую экспертизу по выявлению их содержимого, факта использования вредоносных компьютерных программ. Изучаются сервисы по продажам товаров, предоставлении платных услуг, а также социальные сети, используемые потерпевшим и мошенником.

При производстве следственных действий (осмотре, обыске, выемке) следует обязательно привлекать специалистов в сфере использования компьютерных технологий и программирования. Специалист в ходе осмотра поможет установить принадлежность IP-адреса конкретному лицу, закрепленному за провайдером услуг сети «Интернет», а также осмотреть содержимое персонального компьютера, сделать скриншоты связанных с преступлением сайтов поставщиков товаров и услуг и т. п.

Как уже упоминалось, современные средства мобильной связи (особенно смартфоны) могут выступать в качестве орудия преступления либо служить источником установления фактов, относящихся к искомому событию. С их помощью преступники поддерживают связь, совершают мошеннические действия, побуждают к совершению насилия, экстремизма и террористических актов, свидетели или потерпевшие используют аудио- и видеозапись разговоров, конкретных действий, событий и т. п. Посредством изучения смартфона можно получить информацию о состоявшихся разговорах, так называемых «биллингах», SMS-сообщений, данные о геолокации устройства пр.

Установление особенностей следовой картины конкретного преступления по цифровым следам дает возможность определить способ совершения преступления, его механизм, выдвинуть версии о событии преступления и определить пути и средства поиска компьютерной и иной информации. Положения УПК РФ о проведении следственного осмотра, производстве обыска и выемки позволяют, учитывая специфику, изымать, фиксировать и исследовать цифровые следы преступления.

ГЛАВА II
ТАКТИКА ПОИСКА, ОСМОТРА, ИЗЪЯТИЯ И ИССЛЕДОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ И ЦИФРОВОЙ ИНФОРМАЦИИ СЕТЕЙ ТЕЛЕКОММУНИКАЦИИ, ИНТЕРНЕТА И ИНЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВ

2.1. Тактика осмотра и изъятия компьютерных устройств, технических средств телекоммуникации и иных электронных устройств

Технические средства современной телекоммуникационной связи и интернета по их назначению и функционалу представлены большим разнообразием электронных устройств. К таковым относят компьютеры, серверы, мобильные телефоны (смартфоны), планшеты, смарт-браслеты, электронные книги и т. п.

Компьютеры (от англ. *computer* — вычислитель) делятся на несколько видов: стационарные (настольные), мобильные компьютеры (ноутбуки), переносные компьютеры (смарт-часы, так называемые гаджеты – от англ. *gadget* — приспособление, прибор). Различают корпоративные и персональные компьютеры. Крупные компании, учреждения и интернет-провайдеры имеют серверы — мощные компьютеры, способные обрабатывать большие массивы информации, принимать и выполнять запросы от персональных компьютеров или рабочих станций. Их используют также в качестве файлообменников, облачных сервисов онлайн-хранилищ.

В настоящее время IT-компании предлагают множество онлайн-хранилищ, которые представляю собой так называемые облачные хранилища, позволяющие владельцам хранить свои резервные копии файлов со своего оборудования. В российском сегменте интернета поставщиком бесплатных облачных технологий выступает «Яндекс Диск», который имеет функции автоматической загрузки с телефонов файлов, в том числе фотографий, поддерживает популярные операционные системы. Уничтожение либо поломка смартфона, компьютера не влияет на облачное хранилище. Обращение к ним позволяет получить важную информацию, имеющую значение для раскрытия и расследования преступлений.

К носителям электронно-магнитной информации относят магнитные ленты (видео- и аудиокассеты), карты, оптические диски

(CD-ROM), «флешки» (устройства флеш-памяти со встроенным интерфейсом USB). В целях коммуникации и использования возможностей интернета наиболее распространены смартфоны (iPhone, iOS-смартфоны, Android-смартфоны).

В связи с широким проникновением современных средств коммуникации в профессиональную деятельность и в частную жизнь каждого гражданина, следователь по большинству преступлений, сталкивается с компьютерными системами и средствами мобильной связи. Существует высокая вероятность, что эти средства коммуникации и интернета могут быть использованы как источники криминалистической информации и средства доказывания по уголовному делу. Поэтому следователь должен владеть тактикой поиска, изъятия, фиксации, осмотра и процессуального оформления средств телекоммуникации и интернета и иных носителей электронной информации.

Основной целью осмотра, обыска или выемки средств ИТКС и компьютерных систем по уголовным делам является: выяснение общей обстановки происшествия; установление обстоятельств, позволяющих определить способ совершения преступления и выдвинуть версии; обнаружение, фиксация и изъятие следов компьютерного преступления.

Осмотр места происшествия, проведение обыска и выемки средства ИТКС проводятся по общим правилам осмотра и иных следственных действий. Как известно, в ходе осмотра места происшествия, обыска должны соблюдаться общие принципы проведения этих следственных действий: законности, своевременности, полноты и всесторонности, объективности, методичности, моделирования, активности, единого руководства др. В связи с возможностью уничтожения компьютерной информации особое значение имеет внезапность и оперативность следственных действий, участие специалиста в сфере компьютерных технологий.

При этом должны учитываться ***особенности функционирования предполагаемой или выявленной цифровой информации***, в частности:

1) опосредованность электронной информации, когда цифровая информация может находиться на материальных носителях за пределами места осмотра либо обыска (например, в облачных хранилищах);

2) обезличенность (анонимность) автора или владельца цифровой информации;

3) динамизм, предполагающий техническую возможность преобразования цифровой информации. Трансформацию цифровой ин-

формации в другие формы (аналоговые, скриншоты, текстовый или графический документ и т. п.);

4) потенциальная возможность утраты цифровых следов, а также возможность их восстановления или поиска на других носителях электронной информации, недоступных в момент осмотра или обыска;

5) возможность копирования без утраты содержания копируемой цифровой информации, наличие копий на удаленных друг от друга носителях, доступ к которым могут иметь различные субъекты.

При осмотре объектов компьютерных систем решаются следующие задачи:

1) фиксация индивидуальных признаков (внешнего вида, модели, заводских номеров и иных обозначений на изъятых компьютерах, смартфонах, накопителях электронной информации);

2) определение конфигурации и топологии ИТКС и способа подключения к глобальной сети «Интернет»;

3) установление технических характеристик устройств, каналов связи и вида установленного программного обеспечения;

4) получение данных о провайдере, операторе средств мобильной связи;

5) изучение системных журналов, анализ событий по несанкционированному изменению системных паролей доступа или регистрации новых пользователей;

6) обнаружение и диагностика программ, обеспечивающих несанкционированный доступ, копирование, удаление или модифицирование информации и т. п.;

7) сохранение на внешнем диске, электронном носителе информации следователя и специалиста файлов, производство скриншотов браузеров, снимков экрана отдельных событий, а также их распечатка на бумажном носителе;

8) в зависимости от целей осмотра или обыска, обнаружение и изъятие традиционных следов (например, отпечатков пальцев рук).

Особенности участия специалиста в области компьютерных и информационных технологий. В соответствии с требованиями ст. ст. 182, 183 УПК РФ при изъятии и копировании электронных носителей информации в ходе производства обыска и выемки обязательно участие специалиста. Полагаем, такие же требования должны выполняться при проведении осмотра места происшествия, связанного с осмотром и изъятием средств ИТКС. Специалист может осмотреть и назвать установленные и работающие программы, поисковую

систему, электронную почту, имеющиеся файлы, их название, расположение и др.

Законодатель не определил сферу деятельности специалиста. Подразумевается участие специалиста в области компьютерных технологий. С учетом конкретных обстоятельств дела и местных условий, следователь может самостоятельно решать вопрос об участии специалиста в той или иной сфере IT-технологий. Перечень таких специалистов сравнительно широкий. К специалистам в сфере информационных технологий относят тех, кто разрабатывает, создает и внедряет компьютерные программы и технологии, выполняет настройку и сопровождение программного обеспечения поддерживает информационную базу и компьютерную сеть организаций и предприятий.

Как показывает практика, в качестве специалистов привлекаются сотрудники экспертно-криминалистических подразделений МВД России (в штатах этих структур имеются специалисты в сфере IT-технологий), технические работники других служб МВД (сотрудники Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации — УБК МВД России).

Для этих целей могут привлекаться также компетентные работники контролирующих органов, специалисты IT-компаний, судебные эксперты государственных и некоммерческих экспертных организаций, сотрудники научных и учебных заведений, частные лица. Основное требование — эти лица должны быть компетентны в конкретной компьютерной или операционной системе, иметь соответствующий документ об образовании, официальный сертификат о допуске к такой деятельности.

На месте происшествия могут быть обнаружены самые различные ИТКС и компьютерных устройств: от обычной флэш-памяти накопителя или мобильного телефона, смартфона до мощнейших компьютерных систем и серверов. С учетом наличия электронных носителей информации у значительной части населения, на каждый планируемый обыск или выемку, можно предполагать обязательное изъятие карт флэш-памяти или смартфона. В связи с этим невозможно обеспечить участие специалиста-компьютерщика в каждом случае осмотре места происшествия или проведения обыска, выемки. Поэтому изъятие простейших электронных устройств, как говорилось выше, следователь может производить самостоятельно, достаточно участия специалиста-криминалиста. При этом следователь должен владеть

сравнительно глубокими познаниями в сфере компьютерных технологий, чтобы обеспечить надлежащее процессуальное оформление этих следственных действий. Важно правильно описать, отразить внешние индивидуальные признаки, сохранить электронную информацию, правильно упаковать искомые объекты, а в последующем, при необходимости, осмотреть содержимое электронного носителя информации в кабинете следователя, привлекая для этой цели специалиста.

Алгоритм действий следователя при проведении осмотра или обыска, сопряженных с необходимостью изъятии и изучения ИТКС и содержимого ресурсов интернета.

1. Составить план проведения данного следственного действия (время, место, порядок проникновения, используемые технические средства).

2. Определить состав следственно-оперативной группы (далее — СОГ), проинструктировать участников СОГ. Включить с состав СОГ специалиста в сфере IT-технологий.

3. При необходимости решить вопрос об участии понятых, имеющих общие представления о компьютерах и мобильных средствах коммуникации.

4. Решить вопрос об обеспеченности СОГ средствами криминалистической техники. Поручить специалистам подготовить специальные программно-технические средства.

5. До прибытия принять меры по охране места производства следственного действия либо обеспечить внезапность его проведения.

6. По прибытии на место производства следственного действия ознакомить представителя организации или пользователя ИТКС и интернета с постановлением о производстве обыска или выемки.

7. Установить всех присутствующих лиц, отстранить работающих от компьютерных устройств, предложить им выключить и выдать мобильные телефоны, удалить посторонних лиц.

8. Ознакомиться с местом производства следственного действия и определить возможный порядок его проведения.

9. Объяснить цель проводимого следственного действия, путем опроса сотрудников организации и пользователей ИТКС и компьютерных устройств получить предварительные сведения, которые должны быть учтены при производстве следственного действия.

10. Выяснить порядок доступа к компьютерным устройствам, каким образом и кем ведется администрирование сети.

11. Приступить к рабочему этапу проведения следственного действия.

Особенности тактики осмотра технических средств ИТКС и компьютерных устройств.

Рабочий этап. Необходимо зафиксировать расположение компьютеров в помещениях, иных устройств телекоммуникации, их подключение к интернету и каналам телефонной связи. В ходе осмотра компьютера следует отразить наименование фирмы-изготовителя, модель, идентификационный номер, осмотреть системный блок, определить подключенные внешние устройства, наличие флеш-карт, электронных компакт-дисков. При осмотре работающего компьютера необходимо диагностировать программы, которые выполняются в данный момент. Изучается изображение на экране монитора, которое описывается в протоколе, фотографируется, либо осуществляется видеозапись, специалист производит скриншоты браузера.

В соответствии с требованиями ст. ст. 182, 183 УПК РФ, обеспечивая сохранность рабочих программ и содержимого, произвести копирование информации, хранящейся на жестком диске, на компакт-дискету, флеш-карту, внешний накопитель электронной информации, которыми должен располагать специалист; по просьбе владельца средств ИТКС, если это не воспрепятствует расследованию преступления, на электронные устройства владельца. Все действия по копированию информации фиксируются в протоколе. Работа с копиями позволяет сохранить в неприкосновенности исходную информацию, что является средством защиты от утраты информации при манипуляциях со средствами ИТКС (осмотре, изъятии, транспортировке, проведении экспертиз), а также впоследствии при необходимости производить повторную или дополнительную экспертизу, выключить компьютер и продолжить его осмотр. Отметим, что электронная почта изымается по правилам общей выемки (ч. 31 ст. 183 УПК РФ) или по правилам обыска (ч. 91 ст. 182 УПК РФ).

По указанным общим правилам осматривается как работающий, так и не включенный компьютер. В зависимости от ситуации, после консультации со специалистом, компьютерная сеть может быть включена. Следует привлекать к осмотру пользователя компьютерной сети, который может дать пояснения по поводу совершаемых действий. При этом важно исключить возможность пользователя по уничтожению имеющейся информации.

В зависимости от целей следственного действия, выявить и изъять следы рук на корпусе компьютера, мониторе, клавиатуре, мыши, CD-дисках, «флешках», столе и других объектах. Следует осмотреть документацию, записи, на которых могут быть указаны абоненты, логины, пароли и иная важная информация.

Заключительный этап осмотра, обыска, выемки ИТКС и компьютерных устройств.

При выключении питания требуется корректно завершить все исполняемые в данный момент программы, сохранить относящуюся к делу информацию (файлы, тексты, содержание буферов обмена и др.) на отдельных дискетах, «флешках», иных внешних накопителях электронной информации.

Заключительный этап включает внешнюю фиксацию местонахождения ИТКС и фиксацию наиболее важных элементов электронной информации (установленных программ, файлов, открытых браузеров и др.), которая включает изготовление электронных копий, создание скриншотов, составление актов применения специалистом программ для работы с компьютером, осуществление видеосъемки и фотосъемки, изготовление чертежей, планов и схем и др.

Протокол следственного действия составляется по общим правилам УПК. Важно отразить местонахождение, порядок его проведения, описать индивидуальные признаки. Вместе с тем протокол не должен быть перегружен специальной терминологией, которая впоследствии не будет понятна другим участникам расследуемого дела.

В протоколе осмотра должно быть отражено:

— схема размещения компьютерного оборудования и мест хранения носителей информации;

— порядок подключения к периферийным устройствам и к сетям интернета;

— включена ли аппаратура, открытые программы браузера, имена папок и расположение файлов, вид, наименование и, по необходимости, ее содержание, наименование файлов и содержание дискет и иных носителей электронной информации;

— место обнаружения каждого носителя компьютерной информации, его упаковка, надписи или наклейки на упаковке и иные индивидуальные признаки (царапины, различные повреждения и т. п.);

— используемая специальная аппаратура по исследованию ИТКС, способы копирования, упаковки изымаемой аппаратуры и способы дополнительной фиксации следственного действия;

— опечатывать изымаемые объекты рекомендуется посредством наклеивания скотчем листа бумаги с печатями, подписями следователя и понятых на корпус системного блока, разъемов электропитания и подключения периферийных устройств;

— с техническими средствами и носителями информации следует проявлять предосторожность, хранить в соответствующей упаковке, не производить на корпусах записей и печатей, не подвергать их электромагнитному воздействию, обеспечить безопасную транспортировку ИТКС и т.п.

Поиск, изъятие и осмотр средств мобильной связи (мобильных телефонов, смартфонов).

Статья 164^1 УПК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий» довольно подробно регламентирует основания изъятия и процессуальный порядок работы с ИТКС и компьютерными устройствами. Электронные носители информации изымаются с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации может осуществляться копирование информации. Копирование информации производится на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе следственного действия делается запись.

Законодатель ограничил действия следователя только копированием электронной информации при изъятии электронных носителей, принадлежащих владельцу, по преступлениям, совершенным в связи с осуществлением предпринимательской либо иной экономической деятельностью. Данное ограничение связано с недопустимостью приостановления предпринимательской деятельности. Вместе с теми изъятие электронных носителей информации допускается в случаях, когда:

— вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации;

— изъятие электронных носителей информации производится на основании судебного решения;

— на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

Особенности поиска, изъятия и осмотра средств мобильной связи.

Средства мобильной связи широко используются при подготовке, совершении и сокрытии различных видов преступлений. Содержащаяся в них информация может являться важнейшим источником доказательств. Положения УПК РФ позволяют эффективно обнаруживать и изымать цифровые следы преступления.

Средства мобильной связи на момент изъятия могут находиться у подозреваемого, потерпевшего, свидетеля, в помещении, автомобиле, на открытой местности, на месте происшествия, при производстве личного обыска и обыска помещений. В целях обнаружения мобильных устройств, электронных носителей информации, SIM-карт применяются нелинейные локаторы различных модификаций: «Лорнет», «Orion», «Люкс» и др. Нелинейные локаторы предназначены для обнаружения скрытых радиоэлектронных устройств, аудио- и видеопередатчиков («жучков»), мобильных телефонов. Нелинейный локатор может быть использован для проведения оперативно-поисковых работ на местности, в помещениях и в транспорте.

В ходе осмотра места происшествия, обыска и выемки устройство следует описать и сфотографировать в состоянии, в котором оно находилось. Чаще всего мобильные телефоны, смартфоны изымаются в выключенном состоянии. Вход (включение) в сеть может быть простым и с использованием пароля (кода) доступа, известного пользователю. В процессе изъятия и осмотра на телефон может поступить звонок либо иное сообщение.

В дальнейшем телефон для исключения удаленного воздействия может быть выключен. Это допускается в случаях возможности специалиста и следователя войти в сеть с использованием данного устройства. Оптимальным является помещение устройства во включенном состоянии в упаковку, которая бы исключала соединение с сетью, любо включение в работу специального устройства, блоки-

рующего действие сотовой связи в периметре нахождения устройства. Для этой цели могут быть использованы «мешки Фарадея», изготовленные из гибкой металлической ткани. Они используются для блокирования удаленной очистки или изменения беспроводных устройств, обнаруженных в ходе осмотра места происшествия либо выемки и обыска.

При проведении осмотра средств мобильной связи следователь и специалист могут применять как традиционные технико-криминалистические средства обнаружения, предварительного исследования, изъятия и фиксации следов, так и специальную технику, специальное программное обеспечение для доступа, считывания и хранения компьютерной информации.

Тактика проведения данного следственного действия включает в себя три этапа:

1. Наружный осмотр мобильного телефона и установление функциональных возможностей этого устройства.
2. Осмотр содержания мобильного телефона.
3. Изучение, фиксация значимой информации на бумажный или электронный носитель информации и ее последующее изъятие.

На первоначальном этапе изучается общий вид и техническое состояние. Обращается внимание на общие и частные признаки мобильного телефона. В протоколе фиксируются: модель, серийный номер, материал, из которого мобильный телефон изготовлен, цвет, размер, характеристика клавиатуры, дисплея с описанием изображения и содержания. При описании частных признаков в протоколе должны быть отражены состояние корпуса телефона, клавиш, повреждения, надписи. Особое внимание уделяется IMEI-коду и серийному номеру телефона. IMEI-номер содержит информацию о происхождении, модели, и обеспечивает уникальную идентификацию каждого мобильного телефона и соответствие версии программного обеспечения, инсталлированного в мобильный телефон, разрешенной оператором. Можно узнать IMEI-код, набрав *#06# и сделав вызов оператору. В случаях осмотра смартфон в разделе «Настройки» можно найти общую информацию о телефоне, в том числе номер модели, серийный номер и IMEI. При наличии у смартфона двух SIM-карт будет два IMEI-кода, по одному на каждую SIM-карту.

В случае, если на корпусе телефона имеются наклейки, рисунки, то отмечается их расположение, содержание, цвет, форма т. п. В протоколе отражаются неисправности элементов мобильного теле-

фона. При описании средств необходимо использовать термины, которые определены нормативными актами, технической документацией или разработчиками средств мобильной связи.

Следователь с участием специалиста в ходе производства следственного действия может осуществить копирование информации, содержащейся на электронном носителе информации. В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения и полученные результаты. При этом могут использоваться фотосъемка либо видеозапись. Следственное действие может ограничиться дальнейшим изъятием мобильного устройства, которое в последующем может быть осмотрено в кабинете следователя либо назначена судебная экспертиза. В ряде случаев более полно содержимое мобильного телефона может быть изучено с участием специалиста и применением соответствующей аппаратуры на месте производства следственного действия либо в кабинете следователя или по месту проведения судебной экспертизы.

2.2. Тактика поиска, осмотра, фиксации и изъятия криминалистической информации, содержащейся в технических средствах телекоммуникации, сети «Интернет» и иных электронных устройствах

Процессуальными средствами получения криминалистической значимой цифровой информации являются осмотр места происшествия, осмотр электронных носителей цифровой информации, их осмотр в ходе обыска или выемки, а также результаты судебной экспертизы.

Осмотр содержимого информационно-телекоммуникационных средств и компьютерной информации в сети «Интернет» позволяет целенаправленно вести поиск доказательств, оперативно изучить информационную среду компьютера, мобильного телефона, смартфона или внешнего электронного накопителя информации (оптического диска, USB-накопитель, SIM-карты, Flash-карты памяти и т. п.). Цифровые носители информации могут осматриваться в «полевых» условиях непосредственно на месте их обнаружения или в кабинете следователя, а также по месту производства судебной экспертизы. Для этих целей используются специальные технические устройства и программные комплексы типа «Мобильный криминалист», предлагаются

тактические приемы и методы осмотра компьютерных устройств и внешних носителей цифровой информации.

Правовым основанием для осмотра ИТКС и сетевых информационных ресурсов является наличие сведений (фактических данных) о том, что на техническом устройстве ИТКС, в компьютерном устройстве или удаленном сетевом ресурсе размещена информация, имеющая значение для раскрытия, расследования и предупреждения преступления, либо информация, распространение которой в Российской Федерации запрещено. В качестве последней могут быть: сведения о способах, изготовления наркотических средств, взрывчатых веществ и взрывных устройств; информация о призывах к совершению самоубийства; материалы с порнографическими изображениями несовершеннолетних, объявления о привлечении несовершеннолетних для участия в зрелищных мероприятиях порнографического характера и прочее. В случае обнаружения в сетях интернета такой информации, сотрудники правоохранительных органов должны инициировать закрытие противоправного контента в сети Интернет, проинформировать об этом Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Выделим условно типичные ситуации следственного осмотра, связанного с обнаружением и изъятием компьютерной информации:

— осмотр места происшествия, в ходе которого были обнаружены технические средства ИТКС и компьютерные устройства (стационарные компьютеры, ноутбуки, смартфоны, гаджеты, внешние носители электронной информации;

— целенаправленный осмотр места, откуда был произведен неправомерный доступ (при совершении преступления путем удаленного доступа);

— осмотр технических средств ИТКС и компьютерного оборудования, изъятого в ходе проведения других следственных действий (обыска, выемки в ходе добровольной выдачи устройства, например, во время допроса)

Следственный осмотр технических средств ИТКС и информационных ресурсов интернета в рамках УПК РФ имеет свои особенности и специфику. Во-первых, осматривается особый вид объекта — цифровая информация (телефонные номера и факт переговоров абонентов, SMS-сообщения, веб-сайты, веб-страницы, электронные файлы в виде текстовых сообщений, графика, аудио- и видеофайлы, ав-

томатизированная база и электронные ресурсы, доступ к которым возможен только через сеть «Интернет».

Во-вторых, осматриваемая цифровая информация имеет различные режимы защиты и правовой охраны, связанных с гарантиями основных конституционных прав граждан и юридических лиц, защитой государственных интересов и общественной безопасности и т. п.

В-третьих, при осмотре сетевых ресурсов отсутствует традиционное понимание места происшествия, изучается информационная среда в виртуальном пространстве, которое представляет собой систему ИТКС и интернет-ресурсов. Границы такого осмотра определяются емкостью удаленного электронного носителя информации (например, сервера) либо неопределенным множеством этих носителей, объединенных в единую сеть.

В-четвертых, местом доступа к удаленным данным может быть любая географическая точка с возможностью доступа в сеть «Интернет». При этом могут использоваться стационарный компьютер, ноутбук, смартфон, гаджеты и т. п.

В-пятых, для расследования существенное значение может иметь цифровое устройство, с которого производился удаленный доступ к интернет-ресурсу. На таком устройстве могут сохраняться поисковые запросы, история посещения сайтов, данные о местоположении пользователя, логины и пароли и т. п. В связи с этим нельзя повторно использовать эти устройства для удаленного доступа к интернет-ресурсу в ходе осмотра, поскольку эти действия могут привести к изменениям информационной среды компьютера, смартфона, признанного вещественным доказательством по делу.

В-шестых, цифровая информация отличается высоким уровнем динамичности, подвержена дистанционному изменению и уничтожению с других компьютерных устройств, что должно учитываться при ее поиске, осмотре, фиксации и сохранении в целях расследования преступления. Осмотр технических средств ИТКС и сетевых информационных ресурсов следует отнести к неотложным процессуальным действиям.

В-седьмых, в ходе поиска и осмотра цифровой информации следует учитывать вид и технические характеристики технических средств ИТКС и особенности функционирования интернет-ресурсов. Например, при изучении содержимого мобильного телефона (смартфона) можно получить значительный объем криминалистической и иной информа-

ции о владельце смартфона, его связях, посещаемых страниц Интернета, полученной или направленной информации.

Отметим, что анализ нормативно-правовых актов РФ о правовом режиме и гарантиях обеспечения безопасности позволяет выделить несколько видов информации: общедоступную информацию; информацию, доступ к которой может быть ограничен; недоступную информацию, соответственно, не подлежащую распространению.

В соответствии со ст. 7. Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» к ***общедоступной информации*** относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Статья 9 названного закона формулирует положения по ограничению доступа к информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, составляющей государственную, коммерческую, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

В мобильном телефоне и ином компьютерной устройстве могут быть персональные данные, относящиеся к категории ограниченной доступности, защита которых предусмотрена Конституцией РФ (право на неприкосновенность частной жизни, личную и семейную тайну), законами «О персональных данных», «О банках и банковской деятельности», «О коммерческой тайне» и др.

Согласно ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» к таковым относятся: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы. В соответствии с Указом Президента РФ от 6 марта 1997 г. № 188 (ред. от 23.09.2005) «Об утверждении перечня конфиденциального характера» персональные данные относятся к конфиденциальной информации и представляют собой институт охраны прав человека и гражданина на неприкосновенность частной жизни.

В статье 186 УПК РФ закреплено: «При наличии достаточных оснований полагать, что телефонные и иные переговоры подозреваемого, обвиняемого и других лиц могут содержать сведения, имеющие значение для уголовного дела, их контроль и запись допускаются при производстве по уголовным делам о преступлениях средней тяжести, тяжких и особо тяжких преступлениях на основании судебного решения». Поэтому при изъятии средств мобильной связи следует учитывать, имеются ли в мобильном телефоне сведения, отнесенные к различным видам тайн (личная, семейная, государственная, коммерческая, служебная, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и т. д.), а потому, при необходимости, следователь должен обращаться в суд для получения разрешения на производство осмотра содержимого средств мобильной связи.

Между тем сохраняется правовая возможность проведения органам предварительного следствия изучения содержимого мобильного телефона без судебного решения в рамках осмотра места происшествия. Данная позиция подтверждена определением Конституционного Суда РФ от 8 апреля 2010 г. №433 0-0 «Об отказе в принятии к рассмотрению жалобы гражданина Тарасова Н. А. на нарушение его конституционных прав частью первой статьи 176 и частью первой статью 285 Уголовно-процессуального кодекса Российской Федерации». По определению суда, осмотр места происшествия, местности, жилища, иного помещения, предметов и документов, производимый согласно ч. 1 ст. 176 УПК РФ в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела, осуществляется в предусмотренном законом порядке, в том числе сопровождается составлением соответствующего протокола (ст. ст. 177 и 180 УПК РФ)[1].

[1] Об отказе в принятии к рассмотрению жалобы гражданина Тарасова Николая

Иными словами, в рамках различных видов осмотра в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела, допустим осмотр любой информации, содержащейся в мобильном телефоне, компьютере или ином электронном устройстве.

Положения ст. 164^1 УПК РФ позволяют изымать без судебного решения электронные носители информации в случаях: назначения в их отношении судебной экспертизы; на них содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой по заявлению специалиста может повлечь за собой ее утрату или изменение.

Практика идет по пути использования положений ст. ст. 176, 177,180 УПК РФ об осмотре места происшествия и предметов, положений ст. 164^1 УПК РФ, что позволяет оперативно, без обращения в суд, осматривать мобильные устройства и их содержимое. В процессе осмотра следует применять также правила, изложенные в ст. ст. 182–183 УПК РФ, регламентирующие производство изъятия электронных носителей информации в ходе производства обыска или осмотра места происшествия.

Согласно ст. 161 УПК РФ следователем или дознавателем, в ходе расследования преступления, должны соблюдаться требования о недопустимости разглашения данных предварительного следствия, что является необходимым условием для обеспечения законных прав и интересов владельцев мобильных телефонов, как носителей персональных данных.

Осмотру подлежат имеющие значение для расследования уголовного дела мобильные телефоны, SIM-карты, карты памяти, изъятые в ходе осмотра места происшествия, обыска или выемки либо предоставленные следователю потерпевшими, подозреваемыми и другими лицами. Для надлежащего изучения информационного содержимого средств мобильной связи следователю необходимо обеспечить сохранность обнаруженной компьютерной информации.

Алексеевича на нарушение его конституционных прав частью первой статьи 176 и частью первой статью 285 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда Российской Федерации от 8 апреля 2010 г. №433-О-О. Доступ из справ.-правовой системы «КонсультантПлюс».

В средствах мобильной связи можно обнаружить следующие виды информации: сведения об обслуживающем телефон операторе, тарифе, видах предоставляемых услуг; электронные следы о времени и содержании соединений (сообщений, телефонных разговорах) с другими абонентами или устройствами (серверами), записи в телефонной книге, электронные файлы, фотографии и др. Особое внимание уделяется установленным приложениям мессенджеров и социальных сетей (Viber, Skype, WhatsApp, Facebook, Vkontakte). Подлежит изучению информация на SIM-карте, дополнительной карте памяти, в памяти электронного устройства. Цифровая информация в мобильном телефоне хранится в файлах и представлена в виде текстовой, числовой, графической информации, фотоизображений, видеоклипов и т. д.

При включении мобильного телефона может понадобиться PIN-код, который необходим для доступа к данным SIM-карты. Сведения о PIN-коде известны пользователю и оператору как поставщику услуг мобильной связи. В ходе осмотра владельцу мобильного телефона следует предложить сообщить данные коды, либо получить согласие на разблокирование телефона без его участия и самостоятельно разблокировать свой телефон. При отказе владельца телефона назвать PIN-код, доступ к содержимому телефона может быть произведен специалистом посредством использования специальных технических средств и программного оборудования.

По общему правилу, относящаяся к расследованию преступления электронная информация записывается в протокол осмотра с обязательным указанием последовательности всех действий, произведенных с мобильным телефоном. Фиксируется и процессуально оформляется текстовая, звуковая, фото-, видеоинформация. Изъятие осмотренной информации в мобильном телефоне производится путем ее распечатывания с помощью принтера на бумажном носителе и копируется на отдельный электронный носитель. Фиксация компьютерной информации на электронные носители позволяет обеспечить неизменность и доступность для ее дальнейшего исследования. Скопированные на электронный носитель файлы могут изучаться в дальнейшем с использованием специальных программ, позволяющих ее расшифровывать, анализировать и делать доступной для восприятия участникам уголовного процесса. Соблюдение процессуальных требований гарантирует достоверность и допустимость информации как источника доказательств.

На вооружении правоохранительных органов имеются современные компьютерные криминалистические средства, с помощью которых можно в ходе осмотра места происшествия, обыска извлекать имеющуюся (в том числе удаленную) электронную информацию из памяти электронных устройств. Современные технические средства позволяют извлекать информацию с жестких дисков, мобильных телефонов, карт памяти, SIM-карт и т. д. С использованием возможностей спутниковой навигации устанавливать местонахождение (геолокацию) конкретного электронного устройства в момент разговора или передачи сообщения, определять маршрут перемещения смартфона. Компьютерные криминалистические средства позволяют анализировать контакты участников преступных групп, выявляют информацию о связях интересующих следствие лицах, местах и времени посещения этих мест.

При осмотре и исследовании средств мобильной связи могут быть получены сведения об электронной переписке, данные о незаконных банковских операциях, экстремистские материалы и иная запрещенная к распространению на территории Российской Федерации информация, фото- и видеоизображения. Эти приборы позволяют сохранять связь с выключенными устройствами, преодолевать блокировку и пароли, извлекать также удаленную из памяти устройства информацию.

Такими техническими приборами являются так называемые мобильные криминалисты: АПК UFED (Universal Forensic Extraction Device — универсальное извлечение судебных данных), предназначенное для проведения оперативного исследования средств мобильной телекоммуникации.

Отечественный АПК «Мобильный Криминалист» позволяет получить общую информацию о мобильном устройстве, сведения о контактах и соединениях, ознакомиться с содержимым SMS-сообщений, фотографиями, видео- и аудиозаписями, восстановить удаленные данные, проследить маршруты передвижения владельца телефона. Отчеты создаются в текстовых форматах RTF, PDF, XML и др. Применение программного комплекса «Мобильный криминалист» представляет собой осмотр с элементами криминалистического исследования, по существу производится предварительное компьютерно-техническое исследование электронной информации.

Особенности осмотра электронных страниц в технических средствах ИТКС и сетях Интернета.

Особое значение при расследовании преступлений имеет анализ интернет-контента (контент — это любая информация, выраженная текстом, изображением и любыми другими способами передачи). Современные пользователи, в том числе следователи, имеют достаточный уровень знаний о компьютерной технике, владеют компьютером, средствами мобильной связи, знакомы с интернет-ресурсами и техникой поиска. Поэтому осмотр этой информации может производиться следователем самостоятельно при условии обязательного копирования на электронный носитель информации и сопровождении своих действий фото- или видеосъемкой. Вместе с тем в случаях детального и глубокого изучения сложного информационного содержимого компьютера, мобильного телефона либо информации, размещенной в Интернете, для участия в осмотре следует приглашать специалиста. Следует подчеркнуть, что при неосторожных действиях технически невозможно повредить страницу сайта интернета, кроме случаев, когда эта страница видоизменяется либо удаляется ее создателем.

С позиции криминалистики, в рамках уголовного процесса, разработана тактика осмотра интернет-сайтов, имеющих доказательственное значение. Интернет-сайт может рассматриваться как разновидность иного документа, особенность которого заключается лишь в специфической форме представления компьютерной информации. Электронные документы по содержанию и связи с преступлением могут быть отнесены к иным документам (ст. 84 УПК РФ), которые допускаются в качестве доказательств, если изложенные в них сведения имеют значение для установления обстоятельств, указанных в ст. 73 УПК РФ.

В соответствии со ст. 176 УПК РФ, в целях фиксации и процессуального оформления, производится следственный осмотр страницы в браузере монитора компьютера или смартфона конкретного интернет-сайта. Подготовка к осмотру страницы интернет-сайта предполагает получение соответствующих сведений о существовании искомой информации на конкретном интернет-сайте. Такая информация может быть получена оперативным путем, посредством целенаправленного поиска в сети «Интернет», а также в ходе изучения документов, иной электронной информации, допроса свидетелей, подозреваемых, обвиняемых. Серьезную помощь в этом могут оказать сотрудники ЭКЦ и УБК МВД России, которые занимаются борьбой с преступле-

ниями в сфере компьютерной информации и имеют специальную подготовку и технические средства.

Для этой цели необходим компьютер с соответствующим программным обеспечением и соединенный с интернетом, принтер, фотоаппарат. В соответствии с положениями УПК РФ, к осмотру могут быть пригашены понятые, имеющие общее представление о работе интернета. Для этого может быть использовано специальное программное устройство «Мобильный криминалист».

Поиск соответствующего интернет-сайта осуществляется с помощью поисковых систем интернета. При обнаружении искомого сайта и его контента, с помощью сервисной программы производится ***скриншот*** (от англ. *screenshot*) — снимок с экрана монитора компьютера. При наличии гиперссылок, относящихся к исследуемой информации, посредством скриншота делаются снимки web-страниц гиперссылок. Рекомендуется делать общий снимок всего экрана, а при необходимости производить детальный снимок отдельных фрагментов изображения. Полученные снимки должны быть сохранены на компьютере, с них сделаны копии на внешний носитель электронной информации. Снимки необходимо распечатать, желательно в цвете, на бумажный носитель. В качестве дополнительного средства фиксации можно использовать фотосъемку. Это поможет в последующем быстро вернуться к конкретной информации соответствующего интернет-сайта. Подчеркиваем, что осмотр интернет-сайта должен производиться безотлагательно, поскольку инициатор такой информации может легко ее удалить, в том числе в удаленном режиме.

В протоколе осмотра отражаются действия по поиску и фиксации изображения интернет-сайта. Описываются используемые технические средства, программное обеспечение, компьютер, его местоположение, IP-адрес компьютера, используемая поисковая система, обозначается доменное имя интернет-сайта, а также наименование файла и его текстовое содержание.

Когда интересующая следствие информация располагается на электронной почте, то осмотр возможен по трем основным направлениям:

— осмотр электронной почты на компьютерном оборудовании участника уголовного дела и с его согласия;

— осмотр электронной почты на другом компьютерном оборудовании с использованием пароля и PIN-кода пользователя электронной почты;

— осмотр материального носителя с содержащейся на нем перепиской, полученного от почтового сервиса либо оператора мобильной связи;

— осмотр содержания электронной переписки на бумажном носителе (в данном случае применяются правила осмотра документов).

Электронная почта является значимым источником криминалистической информации, в которой отражается переписка между адресатами. Электронная переписка может осуществляться с компьютеров, ноутбуков, планшетов, смартфонов. Эта переписка может касаться личных отношений, может быть обращена на побуждение лица-адресата для выполнения определенных действий, могут быть даны определенные рекомендации и инструкции. Электронная переписка может осуществляться с компьютеров, ноутбуков, планшетов, смартфонов. Электронная почта может быть дополнительным средством передачи информации, переданной в ходе устных переговоров. В ходе переписки могут быть использованы слова и выражения, которые понятны только участникам переписки.

Осмотр электронной почты, интерфейс которой сформирован с применением web-сервисов, сходен с осмотром web-страниц или интернет-сайта. В рассматриваемом случае также применяется программа обозреватель браузера, демонстрируется отображение страницы с содержимым и фиксируется посредством скриншота (снимка) экрана монитора. В протоколе осмотра отражается время получения (отправления) письма, прилагаемые к нему файлы текстовых (фото,- видеозаписей), при необходимости, дословный текст сообщения, а также отмечаются доменные имена ссылки на файлы, размещенные в интернете.

В ходе изучения и анализа электронной почты можно установить:

— историю переписки, подтвердить факт подготовки, совершения и сокрытия преступления, извлечь информацию, представляющую оперативный интерес (например, на стадии подготовки к совершению преступления, об ином совершенном преступлении);

— интернет-ресурсы, предоставляющие возможность восстановить реквизиты доступа к электронным онлайн-сервисам, платежным системам и платформам цифровой дистрибуции (торговли) и т. д.

В ситуациях, когда сообщение сохранено на платформе сервиса мгновенных сообщений, можно определить и зафиксировать местоположение данного устройства. В рамках осмотров видео- и аудиозаписей, следует отразить время создания, размещения, изменения, продолжительность и содержание записи.

Таким образом, осмотр сайтов и web-страниц электронной почты позволяет проводить поисковые и проверочные действия в рамках предварительного расследования, получать информацию для проведения оперативно-розыскной работы. Подчеркиваем, что в качестве источника доказательств выступает материально зафиксированный и распечатанный на бумажный носитель образ соответствующей страницы web- сайта Интернета. Осматривается именно изображение web-страницы сайта Интернета, скриншот и распечатанная страница выступают в виде дополнительного средства фиксации, позволяющая сохранить цифровую и визуально воспринимаемую информацию, поместить ее в материалы уголовного дела.

Соответственно, в качестве источника доказательств, согласно ст. ст. 74, 83 и 84 УПК РФ, выступают одновременно протокол осмотра документа и документ в виде распечатки образа соответствующей страницы сайта. Протокол осмотра web-страницы в браузере должен содержать сведения, подкрепленные выдержками из текста, описанием иного материала (фотоизображения, аудиовидеозаписи). В последующем, при сохранении искомой страницы на интернет-сайте, суд имеет возможность непосредственно перепроверить полученную информацию путем воспроизведения ее на компьютере суда.

Таким образом, протокол осмотра цифровой информации, расположенной в средствах телекоммуникации, компьютерных устройств, на серверах, в облачном хранилище и сетях интернета должен содержать следующие данные:

1) описание технических средств и программных продуктов, использовавшихся при проведении осмотра;

2) указание на провайдера (компании), которые обеспечивает доступ к сети «Интернет»;

3) маршрут доступа к странице через доменные имена и IP-адрес (уникальный числовой идентификатор устройства в сети «Интернет» по протоколу TCP/IP).

4) при осмотре сетевого информационного ресурса фиксируются: характеристика операционной системы устройства, наименование интернет-браузера и его версия; дата и время осмотра информационного ресурса; адрес места размещения искомой информации (сайта, страницы сайта, веб-чата, базы данных и т. п.); длительность посещения интернет-ресурса в 24-часовом формате исчисления времени (времени начала и завершения следственного действия); название интернет-ресурса и его назначение; имя и фамилия автора текста (изоб-

ражения); контактная информация (электронный почтовый адрес, номер телефона); дословно излагается обнаруженная криминалистическая значимая информация.

Важно отразить всю цифровую информацию либо ее фрагменты в файле, который по окончанию осмотра записывается на отдельный электронный носитель информации (оптический диск, флешкарта, иной электронный накопитель). Электронному носителю присваиваются реквизиты, обозначаются вид и формат, серийный номер. Затем он упаковывается, опечатывается, подписывается участниками следственного действия, помещается в специальное хранилище, обеспечивающее его сохранность и транспортировку;

5) к протоколу осмотра приобщаются созданные в распечатанном виде скриншоты браузера просмотра соответствующих страниц компьютерного устройства и интернета в виде отдельных файлов, записанных на электронный носитель информации и распечатанных на принтере;

6) к протоколу осмотра должен быть приобщен в распечатанном виде результат работы использованных специалистом программ для выхода к требуемому сайту. Специалист также отражает отсутствие постороннего информационного влияния на ход производимого осмотра.

Такой подход позволяет оперативно, в кратчайшие сроки, до назначения судебной компьютерно-технической экспертизы, получить значительный объем криминалистической информации и активно использовать ее для выдвижения версий и организации раскрытия и расследования преступления. С другой стороны, полученная информация позволит более полно определить предмет и объекты судебной компьютерно-технической экспертизы, оптимизировать ее назначение и, соответственно, ускорить ее проведение и получение заключения специалиста.

ГЛАВА III
ТАКТИКА ПОДГОТОВКИ И НАЗНАЧЕНИЯ СУДЕБНЫХ ЭКСПЕРТИЗ ПО ИССЛЕДОВАНИЮ СРЕДСТВ ТЕЛЕКОММУНИКАЦИИ И ИНТЕРНЕТА

3.1. Виды судебных экспертиз по исследованию средств телекоммуникации и интернета

В соответствии со ст. 5 УПК РФ, ст. 9 Федерального закона РФ от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» ***судебная экспертиза*** — процессуальное действие, производимое по постановлению следователя или иного полномочным лица, в установленном законом порядке, состоящее из проведения исследований и дачи заключения по вопросам, разрешение которых требует специальных знаний в области науки, техники, искусства или ремесла, в целях установления обстоятельств, подлежащих доказыванию по уголовному делу.

Как было отмечено выше, в очевидных ситуациях для обнаружения следов преступления производится следственный осмотр технических средств ИТКС и сети «Интернет». Компьютерно-техническая экспертиза назначается в случаях, когда вызывается необходимость обнаружения и исследования неочевидных цифровых следов либо следов, требующих применения сложного программного обеспечения и длительного времени изучения виртуальных следов с участием специалиста. В случаях проведения проверочных действий, доследственной проверки, УПК РФ позволяет назначить такую экспертизу до возбуждения уголовного дела.

Судебная компьютерно-техническая экспертиза (СКТЭ) — это самостоятельный развивающийся род судебной экспертизы. СКТЭ — одна из разновидностей судебных экспертиз, объектами исследования которой являются компьютерная техника, цифровые носители информации, а также сама цифровая информация, расположенная в компьютерной технике и обращаемая в сети «Интернет». Назначается органами предварительного расследования, судами и иными сторонами судебных процессов по уголовным делам, гражданским и арбитражным спорам.

Основная цель СКТЭ заключается в поиске и закреплении доказательств. В качестве целей СКТЭ в рамках уголовного судопроизводства выступают:

— поиск, фиксация и проверка доказательств (цифровых следов) по конкретному делу;

— получение информации для выдвижения и проверки криминалистических версий.

Основными задачами СКТЭ являются:

— фиксация материальных признаков (технических параметров) исследуемого объекта — средств ИТКС и компьютерной техники;

— обнаружение, фиксация, изъятие, исследование, анализ и оценка цифровых следов преступления, совершенного с использованием средств компьютерной техники;

— восстановление измененной либо уничтоженной криминалистической значимой цифровой информации в технических средствах ИТКС и компьютерных устройствах;

— установление тождества между идентифицирующим и идентифицируемым объектом (например, между оригиналом файла и его копией, изъятой в ходе осмотра места происшествия;

— диагностика представленного объекта средств ИТКС в части установления признаков и связей между исследуемыми объектами.

Объектами компьютерно-технической экспертизы могут быть: компьютеры (ноутбуки, планшеты), мобильные телефоны, смартфоны, автоматизированные рабочие станции, сервера, операционные системы, компьютерные программы и приложения, электронные носители информации, файлы и пр.

С учетом видов технических средств и их назначением объекты СКТЭ, можно разделить на несколько групп:

— технические средства или аппаратные объекты: стационарные и портативные компьютеры, периферийные устройства (принтеры, сканеры и т. п.), сетевые аппаратные средства (серверы, рабочие станции, сетевые кабели), интегрированные системы (мобильные телефоны, смартфоны, гаджеты и т. п.), встроенные системы на основе микропроцессорных блоков, комплектующие, карты памяти, жесткие диски и др.);

— программные продукты: операционная система, ее программное обеспечение, программы-утилиты, программные приложения по обеспечению решения конкретных задач, текстовые и графические редакторы, системы управления базами данных и т. д.;

– информационные объекты: текстовые и графические документы в виде файлов, аудио- и видеозаписи, изготовленные с исполь-

зованием компьютерных средств файлы мультимедиа, электронная переписка в электронной почте, в чатах и т. п.

В связи с многообъектностью судебная компьютерно-техническая экспертиза условно классифицируется по следующим родам:

— аппаратно-компьютерная экспертиза;

— программно-компьютерная экспертиз;

— программно-технологическая;

— информационно-компьютерная экспертиза;

— компьютерно-сетевая экспертиза;

— техническая экспертиза средств аппаратно-технической поддержки сетей мобильной связи;

— информационно-компьютерная экспертиза данных о пользователе;

— программно-компьютерная экспертиза средств информационной поддержки сетей мобильной связи;

— нормативно-техническая экспертиза используемого программного продукта и правового регулирования движения информации в сети «Интернет».

По существу, если сгруппировать названные роды экспертиз, можно говорить об аппаратно-компьютерной, программно-компьютерной, информационно-компьютерной и компьютерно-сетевой экспертизах.

В связи с неустоявшейся терминологий в различных экспертных учреждениях экспертизу компьютерной техники и информации называют по-разному: компьютерно-техническая, программно-техническая, кибернетическая, информационно-техническая, информационно-технологическая и пр.

При производстве большинства экспертных исследуются одновременно различные объекты и используются комплексные методы исследования, поэтому в постановлении о назначении судебной экспертизы целесообразно указывать родовое наименование экспертизы и назначать судебную компьютерно-техническую экспертизу. Эксперт, в зависимости от поставленных задач и представленных объектов, решает вопрос об использовании тех или иных методик исследования компьютерных средств, их цифрового содержимого и способов входа в интернет.

В целях формирования единого подхода к используемой терминологии приказом Федерального агентства по техническому регу-

лированию и метрологии от 28 марта 2017 г. № 198-ст утвержден и введен в действие Национальный стандарт судебной компьютерно-технической экспертизы. Национальный стандарт разработан федеральным бюджетным учреждением «Российский федеральный центр судебной экспертизы» при Министерстве юстиции Российской Федерации совместно с федеральным государственным казенным учреждением «Экспертно-криминалистический центр Министерства внутренних дел Российской Федерации», Московским государственным юридическим университетом имени О. Е. Кутафина (МГЮА)» и Следственным комитетом Российской Федерации.

Настоящий стандарт устанавливает термины и определения понятий, применяемые в судебной компьютерно-технической экспертизе. Эти термины рекомендуются для применения во всех видах документации и литературы в области судебной компьютерно-технической экспертизы, распространяются как на государственных судебных экспертов, так и на негосударственных судебных экспертов.

Применительно к общим задачам, представляется возможным выделить идентификационные и диагностические задачи СКТЭ.

К идентификационным задачам можно отнести задачи по установлению, например, автора программного продукта, создателя программы, конкретного файла. В ряде случаев решаются вопросы об отнесении технического средства к классу электронных устройств, конкретного компьютера к определенной модели или поколению, определяется его групповая принадлежность. Имеет место установление целого по его части, например, факта принадлежности конкретного файла к единой базе данных. Важнейшая идентификационная задача решается при установлении источников происхождения цифровой информации, например, установление места, времени, технического средства и других обстоятельства изготовления и хранения конкретной версии программного продукта, его копий в других компьютерных системах и интернет-ресурсах.

При проведении СКТЭ решается широкий круг диагностических задач, в частности: непосредственная диагностика состояния компьютерных устройств, механизма их функционирования, наличия повреждений файловой системы, причины нарушения работы систем ПО устройства, зараженность вирусом, восстановление уничтоженных файлов, реставрация первоначального вида объекта или файловой системы компьютера, текста или изображения на электронных

носителях информации и т. п.

В ходе судебной аппаратно-компьютерной экспертизы проводится исследование:

— персональных компьютеров (стационарных, портативных);

— серверов, периферийных устройств и сетевых аппаратных средств;

— мобильных телефонов, смартфонов, гаджетов;

— комплектующих и компонентов (аппаратных блоков, микросхем и др.);

— микросхем памяти, магнитных и лазерных дисков, флэш-карт и т. п.;

Аппаратно-компьютерная экспертиза отвечает на следующие вопросы: к какой марке, модели относится данное компьютерное устройство; его технические характеристики и функциональное назначение; наличие возможности доступа к данному носителю информации и др.

Программно-компьютерная экспертиза, как следует из ее названия, изучает программное обеспечение. В ходе программно-компьютерной экспертизы исследованию подлежат:

— операционные системы, компьютерные программы, средства разработки и загрузки программ;

— приложения общего и специального назначения, системы управления базами данных, текстовые, графические, презентационные редакторы и т. д.

В ходе программно-компьютерного исследования решаются основные вопросы: реквизиты разработчика и владельца данного программного средства, язык программирования; общая характеристика и функциональное назначение программного обеспечения; каков алгоритм установки и эксплуатации данного программного средства; подвергался ли программный продукт модификации и с какой целью было произведено изменение его функций.

Информационно-компьютерная экспертиза данных является одной из распространенных вариантов судебных компьютерно-технических экспертиз. Целью информационно-компьютерной экспертизы является поиск и анализ информации, созданной пользователем или используемой программой. В ходе этой экспертизы в качестве объектов выступают файлы различных текстовых, графических форматов, аудио- и видеозаписей и иной цифровой информации.

При проведении информационно-компьютерной экспертизы решаются такие типовые вопросы: данные о пользователе компьютерной системы; вид формата носителя информации, его характеристики и параметры; особенности доступа к данным на носителе информации; имеются ли признаки несанкционированного доступа; первоначальное содержание файлов на носителе и др.

Компьютерно-сетевая экспертиза призвана решать такие задачи, как: анализ характеристик аппаратного средства и программного обеспечения; функциональное предназначение сетевого окружения; протокол доступа к информационным данным, выхода в сети «Интернет»; установление обстоятельств события в сети, фактов электронных платежей и использования номеров кредитных карт, сообщений и программ связи в интернете, их содержания и др.

Задачи нормативно-технической экспертизы сводятся к исследованию нормативно-технической документации оборудования, систем и IT-сервисов; договоров и технических заданий на разработку систем и сервисов, проектной и организационно-распорядительной документации. Для проведения нормативно-технической экспертизы могут привлекаться специалисты в области проектирования автоматизированных систем, управления в сфере информационных технологий, криптографии и т. п. Так, примером нормативно-технической экспертизы является экспертиза технического проекта на предмет соответствия обеспечения информационной безопасности требованиям регуляторов (ФСБ России, Роскомнадзора, Центрального банка России), а также экспертиза соответствия проектов требованиям законодательства в области информационной безопасности и защиты информации.

Особо следует выделить судебную компьютерно-техническую экспертизу средств мобильной связи, объектами которой являются фактические данные мобильных телефонов (смартфонов), SIM-карт и иного вспомогательного оборудования (карты памяти, персональные компьютеры, флеш-накопители и т. д.).

При проведении компьютерно-технической экспертизы средств мобильной связи исследуются:

1. Мобильный телефон (смартфон) на предмет установления модели, его технических и функциональных характеристик, диагностики фактического состояния и работоспособности объекта.

2. Программное обеспечение и основные характеристики мобильного телефона, исследование его функциональных свойств, программное обеспечение и его настойки.

3. Информация, содержащаяся в памяти телефона, на SIM-карте телефона, флеш-носителях, свойства и фактическое состояние этой информации, определение времени появления информации и пр.

4. Задачи по восстановлению уничтоженной (стертой) информации.

В случае вовлечения технических средств ИТКС, компьютерной техники и интернета в процесс раскрытия и расследования конкретного преступления, при принятии решения о проведении СКТЭ следует учитывать факторы, определяющие следственную ситуацию, в частности:

— уголовно-правовую оценку расследуемого компьютерного преступления либо иного преступления, связанного с использованием ИТКС и интернета;

— наличие доказательственной и ориентирующей информации, связанной с использованием компьютерных средств;

— техническую возможность сохранения и копирования цифровой информации;

— наличие и возможности специальных технических средств по поиску, фиксации и изъятию криминалистической цифровой информации;

— возможное противодействие посредством уничтожения цифровой информации, в том числе с использованием средств удаленного доступа.

Руководствуясь обозначенными подходами, принимая решение о назначении СКТЭ, представляется возможным выделить следующие типовые следственные ситуации.

1. Расследование преступления в сфере компьютерной информации. Типовой экспертной задачей является диагностирование компьютерной системы, исследование аппаратного, программного и информационного обеспечения, а также действий, связанных с неправомерным доступом к данным, уничтожение, модификация, незаконное использование компьютерной информации и программного обеспечения в преступных целях.

2. Компьютерные устройства выступают как средство совершения преступления. В этих ситуациях основными экспертными за-

дачами являются: диагностирование, выявление и исследование функций программного обеспечения, факт использования в целях совершения конкретных преступлений (мошенничества, незаконного оборота наркотических средств и др.).

3. Компьютерные средства, ИТКС и интернет-ресурсы выступают как источник цифровой криминалистической значимой информации. Основными задачами СКТЭ в таких случаях являются: поиск, фиксация и анализ компьютерной информации с позиции относимости и допустимости доказательств, процессуальное оформление этой информации.

3.2. Подготовка и назначение судебных экспертиз по исследованию средств телекоммуникации и интернета

Взаимодействие следователя с экспертом при назначении судебно-компьютерной экспертизы осуществляется в устной форме обращения следователя за консультацией по следующим вопросам:

— определение рода (вида) экспертизы, решение вопроса о целесообразности назначение комиссионной или комплексной экспертиз;

— формулирование вопросов эксперту;

— подготовке материалов и объектов для экспертизы, подбор образцов для сравнительного исследования;

— выбор экспертного учреждения, эксперта в случае обращения не в экспертное учреждение. Следователи органов внутренних дел для проведения СКТЭ могут обратиться в соответствующие экспертные учреждения МВД России и Минюста России. Кроме того, указанные экспертизы проводят так называемые негосударственные экспертные учреждения, которые располагают необходимой инструментальной базой, имеют в штате сертифицированных специалистов в этой области знаний.

Признав необходимым производство судебной компьютерно-технической экспертизы, в соответствии со ст. 195 УПК РФ следователь выносит мотивированное постановление, в котором указываются основания назначения экспертизы, наименование судебно-экспертного учреждения или конкретное указание эксперта, вопросы, подлежащие исследованию, материалы, предоставляемые эксперту.

В настоящее время перечень вопросов СКТЭ как нового развивающегося рода судебной экспертизы находится в постоянном развитии и уточнении. Это объясняется разнородностью задач СКТЭ, ре-

шаемых экспертом, уровнем методического и инструментального обеспечения исследования объектов СКТЭ, а также разноплановой классификацией самих объектов экспертизы. В настоящее время сформулированы несколько групп вопросов эксперту, связанных с современными возможностями СКТЭ.

Основная группа вопросов касается сущности предмета экспертизы и решаемых задач СКТЭ по исследованию устройства ИТКС. Другая группа решаемых вопросов касается установления и изучения в мобильном телефоне файлов, переписки с определенными лицами, программного обеспечения компьютера, проведенных сеансов и переписки на различных платформах Интернета.

Так, на разрешение судебной компьютерно-технической экспертизы средств мобильной связи могут быть поставлены следующие типовые вопросы:

1. Какова техническая характеристика мобильного телефона (наименование, модель), SIM-карты с логотипом (наименование) и карты памяти (наименование, ее емкость), изъятых в ходе проведения следственного действия (осмотра места происшествия, обыска, выемки).

2. Каково функциональное предназначение средства мобильной связи. Какие мобильные приложения (мессенджеры) установлены на данном мобильном телефоне.

3. С какой базовой станцией данное средство мобильной радиосвязи поддерживает устойчивую радиосвязь.

4. Местонахождение (геолокации) средства мобильной связи в конкретное время.

5. Какие сведения содержатся в мобильном телефоне, SIM-картах, картах памяти.

6. Какие удаленные данные имелись в памяти мобильного телефона и установленной в него SIM-карте.

7. Какие фото- и видеоизображения имеются в памяти мобильного телефона.

8. Каковой содержание переписки в приложениях (мессенджерах) исследуемого мобильного телефона с абонентами и иными контактами, адресаты сообщений.

9. Идентична ли переписка, содержащаяся в мобильном приложении (WhatsApp, Viber, Telegram и др.), переписке, указанной в про-

токоле приложения (содержание, дата и время отправки и получения сообщений).

10. Имеются ли признаки фальсификации, модификации сообщений с использованием специальных программ, иных способов изменения содержания, подмены отправителя или получателя, изменение даты и времени отправки или получения сообщения.

11. Какие файлы (фото, видео или др.) находятся в файловой системе мобильного телефона.

Следует отметить, что при расследовании указанной категории преступлений возникает необходимость назначения идентификационных экспертиз фото- и видеоизображений, аудиозаписей, обнаруженных в средствах ИТКС и компьютерных устройств. Например, при исследовании аудио- и видеофайлов со звуковой речевой информацией может потребоваться назначение комплексной СКТЭ и судебной ***фоноскопической экспертизы*** по идентификации человека по голосу. Для исследования видеозаписей может назначаться судебная ***видеотехническая экспертиза*** — один из видов инженерно-технических экспертиз. Объектом видеотехнической экспертизы могут быть материалы видеозаписи (звукозаписи), видеозаписывающая, звукозаписывающая аппаратура и устройства для воспроизводства видео- и звукозаписей. Видеотехническая экспертиза решает задачи по установлению достоверности мультимедийной записи, на каком конкретно устройстве она выполнена и имеются ли признаки изменения видеосъемки.

Судебно-портретная экспертиза назначается для изучения и идентификации содержащихся в памяти технических устройств ИТКС и компьютеров фотоизображений с определенным лицом (подозреваемым, обвиняемым, потерпевшим).

При общении в интернете участники переписки могут использовать специальную терминологию и выражения. Сотрудники органов внутренних дел в последние годы сталкиваются с распространением запретных текстов и материалов. Переписка может помещаться в интернет-форумах, в социальных сетях, в виде записей на стене и т. д. Особенно это касается блогосферы, размещению в Интернете репостов в виде способа обмена информацией. Репост позволяет перенести запись со страницы группы, сообщества либо с иных страниц пользователей социальных сетей на свою страницу. Нередко в такой информации усматриваются признаки преступного унижения человеческой че-

сти и достоинства, призывы к экстремистской деятельности, развратным действиям, насилию по отношению к людям другой веры, социального положения, национальности и иных преступных проявлений.

Оценку истинного содержания информации в таких текстах могут дать специалисты в области лингвистики. В таких случаях может быть назначена ***судебно-лингвистическая экспертиза.*** Специалисты-лингвисты изучают и оценивают информацию, содержащуюся в опубликованных текстах, видео- и аудиозаписях. Специалисты лингвисты могут определить пол автора текста, его возраст, родной язык, уровень образования, национальную и религиозную принадлежность, культурные и нравственные качества, психологическое состояние и др. В зависимости от поставленных задач к проведению судебно-лингвистической экспертизы привлекаются психологи и филологи. В такой ситуации назначается комплексная ***психолого-лингвистическая экспертиза.***

Важным этапом подготовки к проведению СКТЭ являются действия по предоставлению экспертам качественных материалов в необходимых объемах. В качестве объектов экспертного исследования выступают: материалы уголовного дела, в которых зафиксированы обстоятельства обнаружения, изъятия, осмотра средств ИТКС и иной компьютерной техники: мобильных телефонов, смартфонов, компьютеров, SIM-карт, карт памяти, электронных накопители информации, зарядных устройства, руководств по эксплуатации и др.

Транспортировка технических средств ИТКС на экспертизу, как говорилось выше, по возможности, должна осуществляться в экранированной таре, объекты должны представляться эксперту в неизменном виде, соответствовать их фиксации и упаковке проведенного следственного действия. Для экспертного исследования эксперту необходимо аппаратно-программные инструментальные средства, которые при поведении СКТЭ обеспечивают целостность и неизменность представленной оригинальной информации.

В целом процесс исследования цифровых следов в компьютерных устройствах включает несколько этапов:

— подготовка компьютерно-технической экспертизы и представление объектов на экспертизу. На данном этапе следователем (органом дознания) готовятся объекты (компьютерное оборудование, средства ИТКС, электронные накопители информации), определяется вид СКТЭ, уточняются вопросы, подлежащие разрешению, определя-

ется экспертное учреждение либо конкретный эксперт-специалист по данному направлению, выносится постановление о назначении компьютерно-технической экспертизы;

— предварительное изучение объектов, представленных на экспертизу. Эксперт, которому поручено производство экспертизы, изучает упаковку на предмет ее сохранности, идентифицирует поступившие объекты с объектами, указанными в постановлении о назначении экспертизы. Определяет модель и серийный номер устройства, электронных носителей информации, а также индивидуализирующие признаки (цвет, внешний вид корпуса, наличие надписей, повреждений и т. п.);

— подготовка к исследованию. Получив сведения о модели и иных характеристиках ИТКС, эксперт изучает документацию на устройство, определяет программное обеспечение и технические средства, необходимые для проведения исследования;

— изоляция объекта исследования от возможного взаимодействия устройства с сетями сотовой связи и интернета через программные приложения Bluetooth, Wi-Fi-модуль. Это позволяет исключить внесение изменений в память устройства, например, входящими вызовами, SMS-сообщениями, работой мессенджеров, а также исключить уничтожение цифровых следов посредством удаленного доступа к устройству заинтересованными лицами;

— извлечение данных. Изолировав мобильное устройство от сетей, эксперт посредством программного обеспечения производит извлечение и анализ данных (аппаратно-программных комплексов, цифровых следов, файлов и т. п.). Внешние носители информации (карты памяти, электронные диски, накопители информации, флеш-карты) исследуются каждый отдельно. При исследовании средств ИТКС, карт памяти, содержимого мобильного телефона, компьютера эксперт в целях исследования и сохранения данных может копировать файлы на отдельные электронные носители информации;

— анализ полученной информации и формулирование результатов экспертного заключения. Весь ход и порядок проведения экспертизы, используемые программные продукты и компьютерные устройства отражаются в описательной части экспертного заключения. Выводы эксперта зависят от поставленных задач, полноты и качества представленных объектов, возможностей имеющегося методического и аппаратного оборудования. В ходе производства СКТЭ

эксперт может ходатайствовать о предоставлении дополнительных материалов и объектов. При необходимости следователь может присутствовать при проведении экспертизы. По ходатайству подозреваемого, обвиняемого, потерпевшего они могут принять участие в проведении экспертизы, если это будет способствовать установлению обстоятельств дела.

Таким образом, успех расследования во многом зависит от грамотного изъятия, качества, упаковки, хранения и транспортировки переданных на экспертизу объектов, правильного определения предмета исследования СКТЭ, профессиональных качеств экспертов, методической и инструментальной обеспеченности экспертов.

ЗАКЛЮЧЕНИЕ

Деятельность следователя (дознавателя), сотрудников оперативных подразделений органов внутренних дел, специалистов-экспертов по выявлению, фиксации и исследованию цифровых следов при раскрытии и расследовании преступлений требует нового уровня криминалистических знаний в области цифровых технологий. Внедрение цифровых технологий в практическую деятельность способствует повышению эффективности работы правоохранительных органов, позволяет вовлекать в процесс доказывания значительный объем широко распространенной в современных условиях цифровой информации. Технические средства информационно-телекоммуникационных сетей, компьютерные устройства и интернет-ресурсы являются важнейшим источником криминалистической значимой информации о событии расследуемого преступления, его участниках, подготовке к совершению преступления.

По большинству расследуемых преступлений представляется возможным обнаружить цифровые следы в средствах мобильной связи, в стационарных компьютерах, планшетах, ноутбуках, в сети «Интернет». Особую значимость такая информация имеет по тяжким преступлениям, уголовным делам о готовящихся или совершенных преступлениях против личности, в сфере экономической деятельности, хищениях чужого имущества путем мошенничества, незаконной банковской деятельности, незаконном обороте наркотических средств, экстремизме и терроризме.

Цифровая криминалистика находится в стадии становления и интенсивного развития, совершенствуются аппаратно-инструментальные средства работы с цифровыми следами, развивается и совершенствуется методологическое обеспечение судебной компьютерно-технической экспертизы, в экспертную практику внедряются ее новые виды.

В пособии изложены основные тактические и методические особенности обнаружения электронной информации в виртуальных сетях и на компьютерных устройствах, особенности процессуальной фиксации, изъятия и исследования цифровых следов, порядка подготовки и назначения судебной компьютерно-технической экспертизы.

В настоящее время по проблемам цифровой криминалистики и судебной компьютерно-технической экспертизы издается теоретическая и методическая литература, эти вопросы активно обсуждаются на научных конференциях, методические и информационные матери-

алы помещены на официальных сайтах ЭКЦ МВД России, Российского Федерального центра судебных экспертиз (РФЦЭ) при Министерстве юстиции России, негосударственных судебно-экспертных учреждений.

Следует отметить, что курсанты и слушатели, практические работники органов МВД России обязаны владеть современными информационными технологиями. Обращение к научным и методическим разработкам будет способствовать повышению уровня профессиональной подготовки следователей (дознавателей), сотрудников оперативно-розыскных подразделений, что позитивно скажется на раскрытии и расследовании преступлений.

СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12 дек. 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Российская газета. — 1993. — 25 дек.

2. Уголовный кодекс Российской Федерации : федеральный закон от 13 июня 1996 г. № 63-ФЗ (с изм. и доп. от 15 марта 2023 г.) // Собрание законодательства Российской Федерации. — 1996. — 17 июня.

3. Уголовно-процессуальный кодекс Российской Федерации : федеральный закон от 18 декабря 2001 г. № 174-ФЗ (с изм. и доп. от 1 июля 2021 г. № 294-ФЗ) // Собрание законодательства Российской Федерации. — 2001. — 24 дек. — № 52 (Ч. I).

4. О полиции : федеральный закон от 7 февраля 2011 г. № 3-ФЗ (с изм. и доп. от 11 июня 2021 г. № 170-ФЗ) // Российская газета. — 2011. — 8 февр.

5. Об оперативно-розыскной деятельности : федеральный закон от 12 авг. 1995 № 144-ФЗ (с изм. и доп. от 1 июля 2021 г. № 252-ФЗ) // Собрание законодательства Российской Федерации. — 1995. — № 33. — Ст. 3349.

6. О государственной судебно-экспертной деятельности в Российской Федерации : федеральный закон от 31 мая 2001 г. № 73-ФЗ (с изм. и доп. от 1 июля 2021 г. № 273-ФЗ) // Российская газета. — 2001. — 5 июня. — № 106.

7. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации. — 2006. — 31 июля. — № 31 (Ч. I). — Ст. 3448.

8. О персональных данных: федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации. — 2006. — 31 июля. — № 31 (Ч. I). — Ст. 3451.

9. О безопасности критической информационной инфраструктуры: федеральный закон от 26 июля 2017 г. № 187-ФЗ // Собрание законодательства Российской Федерации. — 2017. — 2006. — 31 июля. — № 31 (Ч. I). — Ст. 4736.

Основная литература

1. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие. — В 2 ч. / А. В. Аносов [и др.]. — Москва : Академия управления МВД России, 2019. — Ч. 1. — 208 с.

2. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под ред. В. Б. Вехова, С. В. Зуева. — Москва : Изд-во Юрайт, 2021. — 417 с.

3. Расследование преступлений в сфере компьютерной информации : учебное пособие / Е. Л. Федосеева, С. В. Мухачев, А. А. Харламова [и др.]. — Екатеринбург : Уральский юридический ин-т МВД России, 2019. — 74 с.

Дополнительная литература

1. Багмет А. М., Бычков В. В., Скобелин С. Ю., Ильин Н. Н. Цифровые следы преступлений : монография. — Москва: Проспект, 2021. — 168 с.

2. Бахтеев Д. В. Особенности фиксации и изъятия криминалистически значимой информации, размещенной в сети Интернет // Российский следователь. — 2017. — № 21.

3. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. — Волгоград : ВА МВД России, 2008. — 404 с.

4. Зазулин А. И. Использование цифровой информации в доказывании по уголовным делам : монография. — Москва : Юрлитинформ, 2019.

5. Карагодин В. Н. Исследования компьютерных информационных процессов в структуре науки криминалистики. Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : сборник статей Международной научно-практической конференции. — Электронные текстовые данные (2,33 Мб). — Москва : Академия управления МВД России, 2018. С. 115–120.

6. Клевцов В. В. Проблемные аспекты изъятия электронных носителей информации при расследовании распространения «дизайнерских» наркотиков с использованием сети Интернет // Российский следователь. — 2015. — № 6.

7. Кучин О. С. Электронные носители информации в криминалистике : монография. — Москва : Юрлитинформ, 2017.

8. Осипенко А. Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. — 2016. — № 3. — С. 85–86

9. Россинская Е. Р. Судебная компьютерно-техническая экспертиза: проблемы становления и подготовки кадров экспертов // Теория и практика судебной экспертизы. — 2008. — № 3 (11). — С. 60–66.

10. Россинская Е. Р. Цифровой след как объект судебной экспертизы : материалы Международной научно-практической конференции / Е. Р. Россинская, А. К. Лебедева, М. С. Чернявская. — Москва : Проспект, 2021. — 272 с.

11. Рудых А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. … канд. юрид. наук / А. А. Рудых. — Ростов-на-Дону, 2020.

12. Сотников К. И. О перспективах цифровизации криминалистических методов и процесса раскрытия и расследования преступлений // Криминалистика. — наука без границ: традиции и новации : материалы всероссийской научно-практической конференции. Санкт-Петербург, 1 ноября 2019 года. — Санкт-Петербург : Санкт-Петербургский университет МВД России, 2020. — С. 283–284.

13. Сотников К. И. Цифровая криминалистика: понятие, место, перспективы : материалы всероссийской научно-практической конференции «Криминалистика — наука без границ: традиции и новации». — Санкт-Петербург : Санкт-Петербургский ун-т МВД России, 26 ноября 2021 г. — С. 224–230.

14. Федотов Н. Н. Форензика — компьютерная криминалистика. — Москва : Юридический Мир, 2007. — 432 с.

Для заметок

Для заметок

Учебное издание

Акиев Арби Русланович,
кандидат юридических наук;
Сотников Константин Иванович,
кандидат юридических наук, доцент,
заслуженный юрист Российской Федерации

ТАКТИКА СЛЕДСТВЕННОГО ОСМОТРА И ИССЛЕДОВАНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ СРЕДСТВ ТЕЛЕКОММУНИКАЦИИ И ИНТЕРНЕТА

Учебно-практическое пособие

Редактор *Великих А. Н.*
Компьютерная верстка *Душкова А. Ю.*
Дизайн обложки *Шеряй А. Н.*

ISBN 978-5-91837-716-1

EDN LBAHYP

Подписано в печать 10.05.2023. Формат 60x84 $^{1}/_{16}$
Печать цифровая. Объем 4,25 п. л. Тираж 100 экз. Заказ № 79/23

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1