Академия управления МВД России

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ, В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ

Учебное пособие

Под ред. Ю. В. Гаврилина и А. В. Победкина

Москва • 2021

УДК 343.14
ББК 67.411
И88

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *М. Ю. Терехов,* кандидат юридических наук, доцент, заместитель начальника кафедры уголовного процесса Московского университета МВД России имени В. Я. Кикотя; *Е. В. Зубенко,* кандидат юридических наук, старший преподаватель кафедры специальных дисциплин Владивостокского филиала Дальневосточного юридического института МВД России.

И88

Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учебное пособие / Балашова А.А., Васюков В.Ф., Гаврилин Ю.В. [и др.] ; под ред. Ю.В. Гаврилина и А.В. Победкина. – Москва : Академия управления МВД России, 2021. – 140 с.

ISBN 978-5-907187-68-9

В учебном пособии на основе обобщения следственной и судебной практики представлены уголовно-процессуальные основы использования информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании, а также криминалистические рекомендации по их обнаружению, фиксации и изъятию. Конкретизированы критерии оценки доказательственной информации на электронных носителях. Обозначены основные направления использования криминалистически значимой информации, полученной при исследовании электронных носителей, в процессе расследования преступлений.

Учебное пособие предназначено для курсантов, слушателей, адъюнктов образовательных организаций системы МВД России, студентов и аспирантов юридических вузов, практических работников органов предварительного следствия и дознания.

УДК 343.14
ББК 67.411

ISBN 978-5-907187-68-9

Авторский коллектив:

Балашова А. А., кандидат юридических наук (Восточно-Сибирский институт МВД России): § 1, 2, 3 гл. 1, § 2 гл. 2;

Васюков В. Ф., доктор юридических наук, доцент (Орловский юридический институт МВД России имени В. В. Лукьянова): § 3 гл. 2, § 1 гл. 2;

Гаврилин Ю. В., доктор юридических наук, доцент (Академия управления МВД России): введение, § 1, 2, 3 гл. 1, § 1, 3 гл. 2, заключение;

Красильников А. В., кандидат юридических наук, доцент (Академия управления МВД России): § 2 гл. 1;

Морозова Н. В., кандидат юридических наук (Орловский юридический институт МВД России имени В. В. Лукьянова): § 3 гл. 2, § 1 гл. 2;

Победкин А. В., доктор юридических наук, профессор (Академия управления МВД России): § 1, 2, 3 гл. 1, § 2 гл. 2.

Оглавление

Введение

Развитие цифровой экономики, совершенствование информационно-телекоммуникационных технологий, их широкое внедрение в сферы государственного управления, бизнеса, а также повседневную жизнедеятельность граждан и организаций является приоритетным направлением социально-экономического развития Российской Федерации на современном этапе. Документы стратегического планирования[1], принятые в период 2014–2020 годов, предусматривают повышение благосостояния, качества жизни и работы граждан, улучшение доступности и качества государственных услуг, повышение степени информированности и цифровой грамотности, развитие экономического потенциала страны с использованием современных информационных, телекоммуникационных и цифровых технологий, являются приоритетными направлениями развития информационного общества в Российской Федерации.

Сегодня на наших глазах активно развивается техническая цифровая инфраструктура, включая сети мобильной связи 5-G, широкополосного доступа в Интернет и др. При этом, на фоне снижения стоимости услуг связи и самих цифровых устройств, растет доступность цифровых услуг, формируются целые отрасли цифровой экономики.

Однако наряду с неоспоримыми достижениями информатизация принесла с собой целый ряд негативных явлений. В их числе риски роста безработицы вследствие высвобождения значительного числа трудоспособного населения за счет автоматизации ручного труда, уязвимость персональной информации от неправомерного доступа к ней, деформация мировосприятия и когнитивные расстройства потребителей цифрового контента, очевидные недостатки дистанционного образования (в виде худшей усвояемости учебного материала, недостатков контроля, качества контента и пр.). При этом в приведенном перечне рисков, сопровождающих развитие цифровых технологий, особо выделяется тенденция цифровой трансформации современной преступности.

Цифровая трансформация преступности выражается в принципиальных изменениях как в механизме совершения «традиционных» преступлений, возникших в «доцифровую» эпоху, так и в возникновении новых видов преступлений, непосредственно связанных

[1] См.: указы Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы», от 1 декабря 2016 г. № 642 «О Стратегии научно-технологического развития Российской Федерации», от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» и др.

с развитием информационно-телекоммуникационных технологий и использованием технических средств сбора, обработки, хранения компьютерной информации и ее передачи по линиям связи.

Следствием цифровой трансформации преступности выступают:

1. Рост числа преступлений, совершенных дистанционным способом, при котором исключается непосредственный контакт субъектов преступления как между собой, так и с потерпевшими. Механизм противоправного воздействия на потерпевших при этом носит опосредованный характер и реализуется с использованием информационно-телекоммуникационных технологий. Последние включают в себя технологии беспроводной связи, передачи информации посредством сервисов электронной почты, обмена мгновенными сообщениями, социальных сетей, систем дистанционного банковского обслуживания и пр.

2. Совершенствование способов сокрытия преступлений, основанных на использовании сервисов анонимизации личности в цифровом пространстве. Анонимизиция направлена на подмену либо блокирование информации, позволяющей установить лицо, совершившее интернет-соединение (прежде всего IP-адрес и MAC-адрес) при отправлении того или иного сообщения посредством электронной почты, сервиса мгновенных сообщений, социальных сетей и пр. Она обеспечивает сокрытие подлинных данных о личности пользователя сети интернет и направлена на воспрепятствование установлению лица, совершающего те или иные действия в виртуальном пространстве, включая противоправные действия.

3. Использование криптовалют в криминальных взаиморасчетах. Сокрытие следов финансовых транзакций активно осуществляется посредством конвертации денежных средств, номинированных в национальных денежных единицах, в виртуальную валюту, оборот которой не подконтролен для уполномоченных государственных органов, что препятствует реализации механизмов противодействия легализации (отмыванию) доходов, полученных противоправным путем, применительно к подобным цифровым финансовым активам.

4. Рост масштабов межрегиональной и трансграничной преступности, использование при совершении преступлений сетевой инфраструктуры, расположенной за пределами Российской Федерации. При этом широкие возможности свободного использования серверных мощностей и информационных ресурсов, расположенных в иностранных юрисдикциях, существенным образом препятствуют установлению лиц, совершивших преступления, и выяснению обстоятельств расследуемого события, подрывая базовый принцип неотвратимости наказания.

5. Использование технологий искусственного интеллекта в противоправной деятельности. В настоящее время широкое рас-

пространение приобрели интеллектуальные технологии синтезирования речи, видеоизображений, с помощью которых можно создавать аудио- и видеозаписи для манипуляции людьми, распространения фальшивых новостей и видеосюжетов. Данные технологии могут быть применены и при совершении преступлений с использованием методов «социальной инженерии».

В этих условиях вопросы выявления, раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, относятся к числу приоритетных направлений деятельности правоохранительных органов. На расширенной коллегии МВД России, состоявшейся 3 марта 2021 года, Президент Российской Федерации В. В. Путин отметил, что за последние 6 лет число преступлений в киберпространстве возросло более чем в 10 раз и указал на необходимость эффективного ответа на этот криминальный вызов, обеспечение защиты граждан и добросовестного бизнеса, который активно осваивает цифровое пространство[1].

Следует подчеркнуть, что в условиях развития информационного общества роль и значение доказательственной информации, содержащейся на электронных носителях, будет неуклонно возрастать, что обусловливает необходимость детального правового регулирования порядка ее собирания и дальнейшего использования в процессе раскрытия и расследования преступлений.

При этом приходится констатировать, что сотрудники органов предварительного расследования допускают процессуальные нарушения и тактико-криминалистические ошибки при обнаружении, фиксации и изъятии электронных носителей, содержащейся на них информации в цифровой форме, в процессе производства отдельных следственных действий, в частности, следственного осмотра, обыска, выемки, допроса, назначения и производства судебной компьютерной экспертизы. При этом правовые последствия подобных нарушений и тактических ошибок весьма велики: от признания протокола следственного действия недопустимым доказательством до невосполнимой утраты доказательственной информации или ее существенной модификации, делающей невозможным дальнейшее экспертное исследование.

В настоящем учебном пособии предлагаются рекомендации, которые позволят должностным лицам органов предварительного следствия и дознания разрешить обозначенные проблемные ситуации.

---

[1] Расширенная коллегия МВД России [Электронный ресурс]. URL: http://www.kremlin.ru/catalog/persons/310/events/65090 (дата обращения: 04.03.2021).

Глава 1. Понятие и правовая характеристика доказательственной информации на электронных носителях

§ 1. Понятие и классификация электронных носителей информации

В основе механизма преступлений, совершенных с использованием информационно-телекоммуникационных технологий, лежат цифровые технологии дистанционной передачи компьютерной информации (данных). Компьютерная информация, как основа доказательственной информации при расследовании рассматриваемых преступлений, обладает комплексом криминалистически значимых свойств, включая быстроту обработки, особый формат данных, способность к пересылке по коммуникационным каналам связи, возможность находиться на носителях особого типа – электронных носителях информации. Названные свойства компьютерной информации обусловливают и особенности электронных носителей информации.

С учетом сказанного представляется целесообразным содержательный анализ понятия, свойств и видов электронных носителей информации предварить рассмотрением особенностей компьютерной информации.

Термин «информация» (от лат. Informatio – разъяснение, представление, ознакомление, понятие) связывается с такими понятиями, как «знания», «сведения», «данные», «сообщения о чем-либо». Так, толковый словарь С. И. Ожегова и Н. Ю. Шведовой определяет информацию как:

1) сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством;

2) сообщения, осведомляющие о положении дел, о состоянии чего-нибудь. Например, научно-техническая и газетная информация; информация средств массовой информации (печать, радио, телевидение, кино)[1].

В настоящее время в научной литературе предлагаются различные подходы к определению понятия информации.

С позиций информатики – науки, занимающейся изучением законов, методов и способов накапливания, обработки, передачи информации с помощью ЭВМ и других компьютерных устройств,

[1] *Ожегов С. И., Шведова Н. Ю.* Толковый словарь русского языка. Москва, 2008. С. 257.

а также различными аспектами применения и разработки последних, – информация представляет собой совокупность знаний о фактических данных и зависимостях между ними, содержание, присваиваемое данным посредством соглашений, распространяющихся на эти данные[1].

А. И. Трусов предлагает определение информации, в основу которого положено отражение как свойство материи: «...информация охватывает отражение предметов и явлений в человеческом сознании, явлений и процессов друг в друге, вне связи с сознанием»[2].

Понятие «информация» зачастую отождествляется с понятием «сведения». Последние представляют собой данные вне зависимости от источника происхождения и материального носителя[3].

Однако при этом следует сделать следующее уточнение. Представляется, что даже исходя из этимологии, «сведения» связаны с осведомленностью, т. е. с осознанным восприятием данных, с получением знания, которое можно использовать в практической деятельности. В этой связи передачу данных влечет любое отражение, однако передачей сведений характеризуется лишь осознанное восприятие данных, которые выступают общим понятием и представляет собой любую информацию, представленную в виде, пригодном для обработки[4].

Таким образом, сведения – это данные об объекте, воспринятые человеком осознанно и осмысленно[5].

Этот подход оптимален для цели исследования уголовно-процессуального доказывания. Информация – только активная форма отражения (сведения), пригодная для практической деятельности[6]. Действительно, вряд ли можно считать информацией данные, которые воспринимающий объект не способен осмыслить и переработать. Отсюда следует, что информация неразрывно связана с целями, стоящими перед объектом, ее воспринимающим. Информация

---

[1] *Першиков В. И., Савинков В.М.* Толковый словарь по информатике. Москва: Финансы и статистика, 1991. С. 129.

[2] *Трусов А.И.* Судебное доказывание в свете идей кибернетики // Вопросы кибернетики и право. Москва: Наука, 1967. С. 20.

[3] Именно так рассматривал понятие «сведения» А.М. Ларин. См.: *Ларин А.М.* Рецензия на книгу «Состязательное правосудие. Труды научно-практических лабораторий / под ред. С.А. Пашина, Л.М. Карнозовой. Вып. 1. Москва, 1996 // Государство и право. 1997. № 10. С. 123.

[4] Информационная безопасность и защита информации: сборник терминов и определений. Москва, 2001. С. 15.

[5] *Победкин А. В.* Уголовно-процессуальное доказывание. Москва: Юрлитинформ, 2009. С. 19.

[6] *Афанасьев В. Г.* Социальная информация и управление обществом. Москва, 1975. С. 34.

осмысливается и трактуется в аспекте той цели, которая стоит перед воспринявшим. Иначе говоря, из одних и тех же данных может быть извлечена разная информация. Учитывая стоящую перед познающим объектом цель, информацию в целом верно определяют как функцию целевой интерпретации полученного сообщения[1], даже если воспринявший ее – ею и не воспользовался[2].

Важной чертой информации является и функция, которую она выполняет в процессе познания: уменьшение неопределенности какого-либо явления, объекта познания, существующей до получения информации[3]. При этом информация не только снимает (уменьшает) неопределенность объекта, но и позволяет выделить его из круга иных, т. е. снимает неразличимость между объектами[4]. Информация, как справедливо замечает Р. М. Ланцман, – это все то, «что отличает одно явление от другого либо характеризует различные состояния одного явления»[5].

Однако для того, чтобы сигнал стал информацией, т. е. явлением, которое снимает неопределенность объекта, от которого сигнал исходит, или его неразличимость, воспринимающий объект должен быть высокоорганизован – до такой степени, которая позволяет работать с полученным сигналом так, чтобы выделить из сигнала (их совокупности) тот смысл, который требуется в связи с целями, стоящими перед воспринимающим объектом. В том случае, когда речь идет о человеке, воспринимающем сигналы, называть его объектом не в полной мере верно, поскольку человек не только воспринимает, интерпретирует сигналы, но и активно влияет на объект, породивший сигнал. В этой связи – человек субъект восприятия информации. В то же время и то лицо, которое информацию передает, – не объект, а субъект информационного процесса, поскольку активно взаимодействует с тем, кто информацию воспринимает. Конечно, высокоорганизованные системы, основанные на информационно-телекоммуникационных технологиях, также способны

---

[1] См., напр.: *Овчинский А. С.* Информация и оперативно-розыскная деятельность. Москва, 2002. С. 16.

[2] Правовая кибернетика социалистических стран: учебное пособие / под ред. Н. С. Полевого. Москва, 1987. С. 101.

[3] *Винер Н.* Кибернетика и общество. М., 1958. С. 31; *Згадзай О. З., Казанцев С. Я., Филиппов А. В.* Информатика и математика для юристов: учебник. Казань, 2000. С. 7.

[4] См. об этом: Правовая кибернетика социалистических стран: учебное пособие / под ред. Н. С. Полевого. Москва, 1987. С. 105; *Бирюков Б. В.* Кибернетика и методология науки. Москва, 1974; *Урсул А. Д.* Проблемы информации в современной науке. Философские очерки. Москва, 1975.

[5] *Ланцман Р. М.* Использование возможностей кибернетики в криминалистической экспертизе и некоторые проблемы уголовно-судебного доказывания: автореф. дис. ... д-ра юрид. наук. Москва, 1970. С. 18.

к активному восприятию информационных сигналов. Однако – они все же объекты информационного процесса, поскольку действуют неосознанно, исключительно в рамках заданных параметров и тех операций, которые заложены человеком (даже если речь идет о сильном искусственном интеллекте). Таким образом, информация характеризует только те процессы, где субъект или объект, ее получающий, организован на уровне, позволяющем воспринимать информационные сигналы, перерабатывать их, интерпретировать в соответствии с поставленными целями, и с учетом этих же целей использовать их. Передача, восприятие, переработка, интерпретация и использование сигнала – содержание информационных сигналов. Сигнал при этом является формой кодировки и передачи информации, т. е. существенных характеристик, которые могут иметь самую различную физическую природу и в информационном процессе выполняют функцию носителя информации от ее источника к приемнику и далее к адресату[1].

Для целей уголовно-процессуального доказывания информацию можно определить как совокупность существенных признаков объекта, выделяющих его из внешней среды и отделяющих от сходных объектов, характеризующие его внутреннее строение (данные об объекте) и существующие в виде сигналов различной физической природы и формы, выполняющих функцию носителя данных к иному (воспринимающему) субъекту, который имеет возможность и обязан эти данные воспринять, переработать, интерпретировать и, при необходимости, использовать в аспекте стоящих перед ним задач[2].

Информационные процессы в уголовно-процессуальном доказывании протекают в форме уголовно-процессуальных отношений. Уголовно-процессуальное доказывание, с точки зрения процесса познания, представляет собой не что иное, как систему информационных процессов. Собственно информационную природу имеют все уголовно-процессуальные отношения. Обмен информацией в них может быть способом формирования доказательств, условием реализации прав участников уголовного судопроизводства, условием реализации обязанности участником судопроизводства и собственно формой реализации прав и обязанностей[3].

---

[1] Правовая кибернетика социалистических стран: учебное пособие / под ред. Н. С. Полевого. Москва, 1987. С. 103.

[2] *Победкин А. В.* Уголовно-процессуальное доказывание. Москва: Юрлитинформ, 2009. С. 22–23.

[3] *Иванов Е. Е.* Уведомление в досудебных стадиях уголовного судопроизводства: автореф. дис. ... канд. юрид. наук. Москва, 2020. С. 11.

Информационные процессы в ходе осуществления уголовно-процессуального доказывания имеют особое значение. Последнее при этом представляет собой сущность уголовного судопроизводства, ради правильного познания значимых для уголовного дела обстоятельств оно и осуществляется. При этом информационные процессы и в рамках иных уголовно-процессуальных отношений служат в конечном итоге интересам правильного познания, даже если речь идет о правоотношениях, выступающих гарантией прав и законных интересов личности.

Информационные процессы осуществляются в рамках реализации прав и обязанностей участников правоотношения. С учетом прав и обязанностей как одной из характеристик правоотношения его участниками являются субъекты, а не объекты. Таким образом, участниками информационных процессов в уголовном судопроизводстве являются субъекты уголовно-процессуальных правоотношений.

На законодательном уровне понятие «информация» впервые было закреплено в Федеральном законе от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации», в котором она определялась как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

В пришедшем ему на смену Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» понятие информации представлено более широко – как «сведения (сообщения, данные) независимо от формы их представления» (ст. 2). Заметим, что с учетом изложенного выше подхода к соотношению понятий «сведения», «информация», «данные» точнее было бы определить информацию как «данные» (сведения и иные данные). Законодатель же сведения, сообщения и данные посчитал понятиями тождественными. В уголовном судопроизводстве информационный сигнал воспринимается, перерабатывается, интерпретируется и используется людьми, т. е. осознанно. Соответственно, информация в уголовном процессе может рассматриваться как синоним сведений.

Одним из видов информации по форме предоставления (наряду с аудиальной, визуальной, тактильной, вкусовой и пр.) является компьютерная информация.

В соответствии с примечанием к ст. 272 Уголовного кодекса Российской Федерации (далее – УК РФ) компьютерной информацией являются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хране-

ния, обработки и передачи[1]. Согласно пункту «б» ст. 1 Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (от 1 июня 2001 г.) компьютерная информация – это «информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи»[2].

Заслуживают внимания и выводы В. Б. Вехова, который определяет компьютерную информацию как сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов[3].

Компьютерной информации присущи следующие особенности[4]:

1. Быстрота обработки, как совокупности операций по ее сбору, накоплению, вводу, выводу, приему, передаче, записи, хранению, регистрации, уничтожению, преобразованию и отображению[5]. Для оценки быстродействия современных информационных систем используется интегральный показатель, учитывающий количество операций вычисления в секунду, операций доступа к памяти в секунду, производительность трехмерной графики, скорость обмена данными с диском и др. Если первые персональные компьютеры осуществляли менее 10 операций с плавающей запятой в секунду, то производительность современных компьютеров оценивается десятками триллионов подобных операций в секунду.

2. Простота уничтожения. Следует отметить, что при удалении файла с использованием штатных средств операционной системы происходит лишь удаление его имени из файловой таблицы,

---

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: заключено в г. Минске 01.06.2001 // Собр. законодательства Рос. Федерации. 2009. № 13. Ст. 1460.

[3] *Вехов В. Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград: ВА МВД России, 2008. С. 234.

[4] *Гаврилин Ю. В.* Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: монография. Тула, 2009.

[5] ГОСТ Р 512775-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения // Консорциум КОДЕКС: Электронный фонд правовой и нормативно-технической документации: сайт. URL: http://docs.cntd.ru/document/1200025597/ (дата обращения: 28.10.2019).

сама же информация остается неизменной, что позволяет легко восстановить удаленные таким способом данные. В этой связи в настоящее время широкое распространение получили специальные программные и физические методы удаления компьютерной информации без возможности последующего восстановления. Первые основаны на многократной перезаписи новой информации на месте старой. Вторые осуществляются путем механического воздействия на носитель информации ионизирующего излучения, многократного размагничивания и намагничивания рабочего слоя носителя и другими методами[1].

3. Возможность создания, изменения, копирования с помощью средств компьютерной техники. Последняя осуществляет преобразование информации в двоичный код – последовательность нулей и единиц, что обусловливает возникновение термина «цифровая информация». В процессе создания цифровой информации возникает новая запись на электронном носителе. Модификация цифровой информации означает внесение в нее изменений (или в ее параметры). Копирование цифровой информации представляет собой ее перенос на обособленный носитель при сохранении неизменной первоначальной информации[2].

4. Способность к передаче по телекоммуникационным каналам связи компьютерных сетей на любое расстояние. В последнее время получили широкое распространение технологии проводной и беспроводной пакетной передачи данных, широкополосного доступа в сеть Интернет. Активно развиваются технологии сотовой подвижной связи, которые эволюционировали от поколения 1G, со скоростью передач данных до 220 Кбит/с, до поколения 5G, со скоростью передачи данных до 10 000 Мбит/с.

5. Возможность одновременного доступа к компьютерной информации нескольких пользователей. Многопользовательские системы управления базами данных, облачные технологии, локальные вычислительные сети, глобальная сеть Интернет – вот далеко не полный перечень средств, обеспечивающих одновременный доступ к информации множества пользователей в соответствии с их правами в информационной системе.

С развитием дистанционных способов совершения преступлений широкое распространение получили тайниково-закладочные

[1] *Бакланов В. В.* Введение в информационную безопасность. Направления информационной защиты. Екатеринбург: УрГУ, 2007.

[2] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации от 30.05.2014 // Доступ из информ.-правового портала «Гарант».

способы незаконного сбыта запрещенных к гражданскому обороту объектов. Так, одна из интернет-платформ, созданная в 2016 г., функционирующая в неиндексируемом сегменте Интернета, осуществляет услуги по реализации не только наркотических средств и психотропных веществ, но и фальшивых купюр, банковских карт, поддельных документов, специального оборудования для слежения, доступа к компьютерной информации и т. д. Платформа содержит в себе интернет-магазины, предлагающие запрещенные к гражданскому обороту товары и услуги, а также предложения о трудоустройстве.

6. *Способность к дублированию*. Содержание любой информации в целом, и компьютерной информации в частности, не зависит от типа используемого для ее хранения материального носителя. Так, при копировании файлов с жесткого диска персонального компьютера на флеш-накопитель, с точки зрения своего содержания, информация на носителе, содержащем ее оригинал и копию, будет идентична. Обозначенное свойство обеспечивает равное доказательственное значение информации и изготовленной с нее копии вне зависимости от типа используемого для ее записи носителя. Как отмечает М. А. Митрофанова, носитель электронного документа всегда может быть заменен на другой носитель без изменения его содержания[1]. Я. А. Карев по этому поводу указывает, что «при совершении сделок путем обмена документами посредством электронной связи замена носителя электронного документа происходит минимум два раза – в момент передачи документа его составителем в информационную систему и в момент его получения адресатом»[2].

Переходя непосредственно к анализу понятия «электронный носитель информации», необходимо отметить следующее.

В настоящее время законодатель использует термин «электронный носитель информации» в тексте Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) более 10 раз. Данная правовая категория была введена в уголовно-процессуальное законодательство с принятием Федерального закона от 28 июля 2012 г. № 143-ФЗ. Несмотря на значительное время, прошедшее со дня принятия названного закона, легальное определение данного понятия по-прежнему отсутствует, что способствует возникнове-

[1] *Митрофанова М. А.* Электронные доказательства и принципы непосредственности в арбитражном процессе: дис. ... канд. юрид. наук. Саратов, 2013.

[2] *Карев Я. А.* Электронные документы и сообщения в коммерческом обороте. Москва, 2006. С. 33.

нию правовой неопределенности и порождает активную научную дискуссию относительно его содержания.

При этом сам термин «электронный носитель информации» также носит дискуссионный характер. Так, по мнению А. И. Зазулина, «использование в УПК РФ термина «электронный носитель информации» необоснованно сужает круг предметов, в отношении которых может быть осуществлено изъятие (при участии специалиста) и копирование компьютерной информации». С учетом изложенного, вышеуказанным автором предлагает ввести в УПК РФ более общий термин – «цифровой носитель информации», включающий в себя различные типы носителей цифровой информации[1]. Представляется, что предложенный А. И. Зазулиным термин является более подходящим, поскольку более точно отражает форму содержащихся на таком носителе данных.

Весьма удачный подход к определению понятия «электронный носитель информации» предлагает Ю. Н. Соколов, понимая под ним технически и технологически адаптированное к многократному использованию электронное устройство, предназначенное для записи, хранения, передачи и воспроизведения электронной информации с помощью доступных технических средств, а также защиту, обособление и разграничение доступа к имеющейся информации. В целом приведенное определение, на наш взгляд, раскрывает сущностные характеристики рассматриваемого понятия, однако выражение «с помощью доступных технических средств» ввиду неопределенности своего содержания нуждается в уточнении.

На правовую сторону вопроса обращают внимание В. Н. Григорьев и О. А. Максимов, которые считают, что «электронный носитель информации» представляет собой особую группу вещественных доказательств и определяют его как «предмет, содержащий значимую для уголовного дела информацию, созданную не в процессе расследования уголовного дела, восприятие которой невозможно без использования электронно-вычислительных средств»[2]. Анализируя приведенное определение, следует заметить, что карта памяти, содержащая информацию, созданную в процессе расследования, включая указанные выше файлы фотоснимков с места происшествия, не перестает быть вследствие этого обстоятельства электронным носителем

[1] *Зазулин А. И.* Обоснованность использования термина «электронный носитель информации» в уголовно-процессуальном кодексе Российской Федерации» // Правопорядок: история, теория, практика. 2016. № 4 (11). С. 56.

[2] *Григорьев В. Н., Максимов О. А.* Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. № 2 (84). С. 40.

информации. К тому же существует большой массив информации, не содержащейся на электронных носителях, восприятие которой невозможно без использования электронно-вычислительных средств. Так, применяя для исследования состава вещества газовый хроматограф, эксперт с использованием данного электронного устройства воспринимает информацию, не содержащуюся на электронном носителе. Кроме того, информация, содержащаяся на электронном носителе, по содержанию может свидетельствовать о его принадлежности к группе иных документов, а не только вещественных доказательств.

По данному вопросу И. С. Федотов и П. Г. Смагин верно отмечают, что «безусловно к электронным носителям информации можно отнести устройства хранения данных (накопители на жестких магнитных дисках, флеш-накопители, компакт-диски и др.), однако на современном этапе развития устройств хранения и воспроизведения информации последняя содержится и в ряде предметов, которые, на первый взгляд, к электронным носителям информации отнести можно весьма условно. К их числу относятся электронные планшеты, сотовые телефоны, плееры, а также «умные» холодильники, бортовые компьютеры автомашин и др.»[1]. К сказанному стоит добавить, что значительный массив информации формируют устройства, относящиеся к «интернету вещей» – изделия хозяйственно-бытового назначения, обладающие элементами искусственного интеллекта. Речь при этом идет, например, о холодильнике, способном самостоятельно осуществлять заказ продуктов питания по мере их потребления, пылесосе, способном самостоятельно выполнять уборку помещения без участия человека, и пр. Очевидно, что информация, которой «обмениваются» подобные устройства, не может находиться вне электронных носителей и коммуникационных каналов связи.

Заслуживает внимания определение, содержащееся в ГОСТ 2.051-2013 «Единая система конструкторской документации (ЕСКД). Электронные документы», согласно которым электронный носитель представляет собой материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники[2].

---

[1] *Федотов И. С., Смагин П. Г.* Электронные носители информации: «вещественные доказательства» или «иные документы» // Вестник ВГУ. Серия: Право. 2014. № 3. С. 195.

[2] См.: ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения // Консорциум КОДЕКС: Электронный фонд правовой и нормативно-технической документации: сайт. URL: http://docs.cntd.ru/document/ (дата обращения: 12.06.2018).

Приведенное определение расширительно толкует рассматриваемое понятие, поскольку позволяет относить к электронным носителям все устройства, реализующие функцию записи[1], хранения и воспроизведения информации, включая широкий спектр предметов хозяйственно-бытового назначения, имеющих в своем составе микросхемы памяти, что не способствует точности при использовании данного термина и может порождать ошибки правоприменения[2].

Итак, сущностным свойством электронных носителей информации является их конструктивная предназначенность для относительно продолжительного хранения данных в цифровом формате для целей их использования в микропроцессорных устройствах. С учетом сказанного, *электронный носитель информации* следует определить как техническое средство, конструктивно предназначенное для хранения информации в электронно-цифровой форме, доступной для обработки с использованием средств вычислительной техники[3].

Характерным признаком электронных носителей информации является их способность сохранять значительный объем информации при относительно малых его физических габаритах. Емкость носителя, измеряемая в Мегабайтах (Мбайт, 1024 Кбайт), определяется прежде всего технологией записи на него информации, которая основывается на следующих физических принципах:

– намагниченность доменов на поверхности магнитных дисков;

– нанесение углублений на поверхности оптического диска, рассеивающих падающий луч лазера;

– передача импульсов по соединительным кабелям от одного компьютера к другому;

– помещение электрических зарядов в электронные «ловушки» полупроводниковой структуры и др.

Приведенный перечень технологий хранения информации не является исчерпывающим. При этом их вариативность оказывает непосредственное влияние на уголовно-процессуальный порядок работы с рассматриваемыми объектами в процессе производства по уголовным делам, особенно на досудебных стадиях уголовного

---

[1] В настоящее время наибольшее распространение получила запись информации на электронные носители информации с использованием различных физических процессов: намагничивания ферромагнетиков в магнитном поле, создания с помощью лазерного луча дорожки в виде спирали, идущей из центра к краю диска, подачи напряжения на управляющий затвор микросхемы памяти и др. См.: *Сенкевич Г.Е.* Искусство восстановления данных. СПб.: БХВ-Петербург, 2011.

[2] *Гаврилин Ю.В.* Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4 (44). С. 48.

[3] *Балашова А.А.* Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. ... канд. юрид. наук. Москва, 2020. С. 41.

судопроизводства. Это влияние вызвано требованием обеспечения достоверности доказательств и неизменности информации, имеющей значение для объективного установления обстоятельств расследуемого события.

Так, совершенно очевидно, что процессуальный порядок изъятия информации, находящейся на флэш-накопителе, не тождественен порядку изъятия информации, находящейся в децентрализованный информационной системе или на сервере, обеспечивающем работу сайта в сети Интернет. Собственно говоря, различные в зависимости от информационного сигнала виды информации обусловливают соответствующую процессуальную форму вовлечения ее в уголовное судопроизводство. В многоэлементной системе процессуальных способов собрания доказательств каждый такой способ предназначен для придания статуса доказательств строго определенному информационному сигналу[1].

Соответственно, для разработки такого процессуального порядка собирания доказательств на электронных носителях информации, который обеспечивал бы достоверное отражение в материалах уголовного дела цифровой информации, содержащейся на электронных носителях, требуется классификация последних, которая может производиться по различным основаниям, в частности:

– **по характеру связи с расследуемым событием** электронные носители информации подразделяются на первичные, то есть непосредственно связанные с событием преступления и иными элементами предмета доказывания (ст. 73 УПК РФ), и вторичные, то есть полученные в ходе процессуальных действий, совершаемых с первичными электронными носителями. Данная классификация основана на выделении в науке уголовного процесса первоначальных и производных доказательств.

В качестве примера первичных электронных носителей информации можно привести их оригинальные экземпляры, содержащие информацию, запись которой была произведена в процессе подготовки, совершения или сокрытия преступления, либо при иных обстоятельствах, имеющих значение для уголовного дела, однако возникших вне связи с процессом расследования.

Вторичные носители содержат копию информации, содержащейся на первичных электронных носителях, полученную в процессе выполнения процессуальных действий с первичными носителями. Так, например, жесткий диск сервера, на котором находится

[1] См., напр.: *Шейфер С. А.* Использование непроцессуальных познавательных мероприятий в доказывании по уголовному делу // Государство и право. 1997. № 9. С. 57–64.

база данных программы автоматизации бухгалтерского учета, является первичным носителям информации, а съемный жесткий диск, на который было выполнено копирование содержимое этого жесткого диска в ходе выемки, будет являться вторичным;

– **по способу использования и получения доступа к содержащейся на электронных носителях информации** последние подразделяются на локальные и сетевые. Использование локальных носителей информации не требует задействования сетевой инфраструктуры и каналов связи. Они могут являться интегрированными элементами информационной системы, либо могут быть физически подключены к соответствующему считывающему устройству или информационному порту. Примером локальных, то есть встроенных, или непосредственно подключаемых к информационной системе электронных носителей информации, служат CD-, DVD-диски, флеш-карты, съемные жесткие диски, а также жесткие диски персональных компьютеров, встроенная память ноутбуков, смартфонов, электронных книг и прочих устройств, для которых хранение информации является одной из функций.

Сетевые носители информации используются путем опосредованного (дистанционного) соединения с использующей их информационной системой по каналам связи. Чаще всего они представляют собой серверы, доступ к которым обеспечивается дистанционно, через компьютерную сеть (как правило, сеть Интернет). Место их физического нахождения, даже если оно находится за пределами юрисдикции Российской Федерации, не имеет значения и не является препятствием для получения доступа к содержащейся на них информации. Чаще всего на удаленных серверах размещаются информационные ресурсы интернет-сайтов, включая получившие широкое распространение социальные сети (Одноклассники, ВКонтакте, Instagram и др.), сервисы обмена сообщениями, электронной почты, электронных торговых площадок и пр. Ключевой особенностью сетевых носителей информации является возможность получения дистанционного доступа к находящейся на них информации посредством специального программного обеспечения, каналов связи, а также услуг специализированных организаций – провайдеров, обеспечивающих распространение информации в сети;

– **по возможности перемещения в пространстве** электронные носители подразделяются на стационарные (настольные компьютеры, моноблоки и т. п.), специально не предназначенные для перемещения в пространстве, и портативные (ноутбуки, нетбуки, планшеты, смартфоны), в том числе съемные носители информа-

ции, включая флэш-карты, конструктивно предназначенные для перемещения.

Стационарные носители информации (персональные компьютеры) отличаются тем, что их перемещение невозможно без частичного демонтажа (отсоединения) периферийного оборудования.

Портативные же носители конструктивно предусматривают возможность их перемещения в пространстве или переноса данных, например флэш-накопитель (USB-диск, карта памяти), оптический диск (лазерный диск, компакт-диск) и пр.;

– **по сроку хранения информации:** носители оперативного хранения (в течение срока определенного информационного процесса), временного хранения (в течение определенного временного интервала), постоянного хранения (неограниченно).

Носители оперативного хранения информации предназначены для оперативного хранения информации и быстрого обмена данными, используемыми в процессе ее обработки. *Они* непосредственно связаны с центральным процессором и предназначены для данных, оперативно участвующих в выполнении арифметико-логических операций[1]. Конструктивно они выполнены в виде отдельных микросхем, расположенных на материнской плате.

Носители временного хранения информации позволяют хранить данные относительно продолжительное время без внешнего энергопотребления, за счет внутренних источников питания (смартфоны, ноутбуки, планшетные компьютеры, иные микропроцессорные устройства, имеющие режим гибернации – минимизации энергопотребления, с возможностью приостановки протекающих в системе информационных процессов);

– **по возможности автономной работы:** энергозависимые (не способные выполнять функцию хранения информации без внешнего энергопотребления) и энергонезависимые (способные хранить информацию без внешнего энергопотребления). При отключении электропитания информация, содержащаяся на энергозависимых носителях информации, пропадает (уничтожается). К ним относится, в частности, оперативное запоминающее устройство (оперативная память) персональных компьютеров. К энергонезависимым носителям относится так называемая внешняя память (жесткие диски, дискеты, лазерные диски, флэш-накопители), обе-

[1] См.: ГОСТ 25492-82 Устройства цифровых вычислительных машин запоминающие. Термины и определения // GOSTRF.COM: сайт. URL: http://gostrf.com/normadata/1/ 4294828/4294828953.htm (дата обращения: 24.09.2019).

спечивающие возможность долговременного хранения информации без потребления электроэнергии.

В литературе встречаются также классификации электронных носителей и по иным основаниям. Так, В. Б. Вехов по целевому назначению выделяет[1]:

– машинные носители информации (ферромагнитная полимерная лента (полоса), гибкий полимерный или жесткий магнитный диск, жесткий оптический или магнитооптический диск и др.);

– интегральные микросхемы (идентификационные модули для сотовых телефонов (SIM-карты), микроконтроллеры (устройства на технологии PayPass, USB-устройства, Flash-карты и др.), электронные вычислительные машины (компьютеры, активное серверное оборудование, банкоматы, терминалы, контрольно-кассовые машины, сотовые радиотелефоны, ресиверы, видеорегистраторы и др.);

– комбинированные носители информации (платежная карта с магнитной полосой и интегральной микросхемой и т. п.), информационные системы, в том числе поисковые, информационно-телекоммуникационные сети, например сеть Интернет.

Вместе с тем последняя представленная классификация не оказывает существенного влияния на уголовно-процессуальные особенности собирания доказательственной информации на электронных носителях информации.

В заключение настоящего параграфа отметим следующее.

Электронный носитель информации представляет собой техническое средство, конструктивно предназначенное для хранения информации в электронно-цифровой форме, доступной для обработки с использованием средств вычислительной техники.

Процессуальный порядок обнаружения, фиксации и изъятия доказательственной информации, содержащейся на электронных носителях, находится в прямой зависимости от вида (типа) такого носителя, технологии доступа к находящейся на нем информации, а также правового режима данной информации.

Классификация электронных носителей информации, определяющая содержание уголовно-процессуального порядка собирания содержащейся на них доказательственной информации, производится по следующим основаниям:

– по характеру связи с расследуемым событием: первичные и вторичные;

---

[1] *Вехов В. Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград: ВА МВД России, 2008. С. 87.

– по способу использования и получения доступа к содержащейся на них информации: локальные и сетевые;

– по возможности перемещения в пространстве: стационарные и портативные;

– по сроку хранения информации: оперативного, временного и постоянного хранения;

– по возможности автономной работы: энергозависимые и энергонезависимые.

Вопросы для повторения

1. Понятие и сущность информации.
2. Понятие сведений.
3. Информационная природа уголовно-процессуальных отношений.
4. Значение информации в уголовно-процессуальном доказывании.
5. Зависимость процессуальной формы от физической природы информационного сигнала.
6. Понятие и характерные свойства компьютерной информации.
7. Существенные признаки электронных носителей информации.

Практическое задание

Используя рассмотренную в настоящем параграфе классификацию электронных носителей информации, определить, к какой классификационной группе относятся следующие объекты:

– карта памяти фотокамеры, принадлежащей подозреваемому;

– флеш-накопитель, изъятый в ходе обыска;

– CD-R диск, содержащий фото с осмотра места происшествия;

– смартфон потерпевшего, на который пришло SMS-сообщение о неправомерном списании денежных средств с банковского счета.

§ 2. Электронные носители информации в системе видов доказательств.

Учение о доказательствах и доказывании традиционно занимает центральное место в науке уголовного процесса. Понятию доказательств в уголовном судопроизводстве посвящены работы В.Д. Арсеньева, Ю.В. Астафьева, О.Я. Баева, А.Р. Белкина, Р.С. Белкина, А.И. Винберга, А.Г. Волеводза, Б.Я. Гаврилова, Г.Ф. Горского, А.А. Давлетова, Е.А. Доли, Н.В. Жогина, В.И. Зажицкого, Д.В. Зотова, Р.В. Костенко, Л.Д. Кокорева, В.А. Лазаревой, П.А. Лупинской, Н.П. Майлис, А.В. Победкина, М.С. Строговича, Ф.Н. Фаткуллина, Л.Г. Шапиро, С.А. Шейфера, П.С. Элькинд и других ученых.

Согласно ст. 74 УПК РФ доказательствами являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном уголовно-процессуальным законом, устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела[1].

Современным представлениям о понятии доказательства и процессе доказывания предшествовала длительная эволюция как предмета, так и средств доказывания.

Знаковыми вехами в процессе эволюции теории доказательств являлись такие памятники права, как Русская Правда, Судебник 1550 года, Краткое изложение процессов – Приложение к Воинскому уставу, принятому в период правления Петра, Свод законов Российской Империи 1825 года и др.

Устав уголовного судопроизводства 1864 года определял понятие «доказательство» как элемент действительности, передающий информацию о свершившемся событии. Доказательствами признавались устные свидетельства и письменные документы, позволяющие обна-

[1] Заметим, что законодатель не в полной мере точно определяет обстоятельства, подлежащие доказыванию по уголовному делу. Они не исчерпываются обстоятельствами, указанными в ст. 73 УПК РФ. Доказыванию подлежат также доказательственные (промежуточные факты), а также обстоятельства, основываясь на которые принимается целый спектр уголовно-процессуальных решений (применение мер процессуального принуждения, производство следственных действий, рассмотрение жалоб на действия должностных лиц, осуществляющих досудебное производство по уголовному делу, и др.). В этой связи в ч. 1 ст. 74 УПК вполне достаточно было бы указать, что на основе доказательств устанавливаются обстоятельства, имеющие значение для уголовного дела.

ружить и изобличить виновного в совершении преступления[1]. Настоящей революцией в уголовном судопроизводстве стало правило о свободной оценке доказательств, предусмотренное в указанном Уставе.

Развитие доктринальных представлений теории доказательств в Российской Империи связано с именами Я. И. Баршева, Л. Е. Владимирова, М. В. Духовского, В. Д. Спасовича, И. Я. Фойницкого и других видных юристов того времени.

Я. И. Баршев определял доказательства через внутреннее убеждение суда в действительности того или иного события. Он делил доказательства на две группы, которые получались непосредственно судом и следователем, на основании чего у них и формировалось внутреннее убеждение в существовании факта, который должен послужить основанием для судебного приговора[2].

Значительный вклад в развитие теории доказательств внес Л. Е. Владимиров, который определял данное понятие через понятие «факт», назначением которого является формирование у судьи убеждения в существовании или в отсутствии существования какого-либо обстоятельства, составляющего предмет судебного исследования[3].

И. Я. Фойницкий понимал доказательство в уголовном судопроизводстве в двух аспектах: во-первых, как средства, служащие для того, чтобы при их помощи сделать заключение об искомом; во-вторых, как сам умственный процесс, путем которого обстоятельство искомое становится в связь с обстоятельством известным, данным и показывается им[4]. Таким образом, И. Я. Фойницкий стал одним из тех специалистов, которые заложили отношение к доказыванию как не только к информационному, но и как к логическому процессу.

М. В. Духовской относительно понятия доказательств отмечал, что ими может быть все, что способно содействовать разъяснению уголовного преступления, невиновности или степени виновности обвиняемого[5].

Начало советского периода в истории уголовного судопроизводства России ознаменовано изданием инструкции Народного Комиссариата Юстиции РСФСР «Об организации и действии местных районных судов» от 23.06.1918, ст. 34 которой определяла, что

---

[1] Устав уголовного судопроизводства от 20.11.1864 [Электронный ресурс] // Доступ из информ.-правового портала «Гарант».

[2] *Баршев Я. И.* Основания уголовного судопроизводства с применением к российскому уголовному судопроизводству. Москва: ЛексЭст, 2001. С. 52, 53.

[3] Учение об уголовных доказательствах. Части: Общая и Особенная / Л. Е. Владимиров. 3-е изд., изм. и законч. Санкт-Петербург, 1910.

[4] *Фойницкий И. Я.* Курс уголовного судопроизводства. Санкт-Петербург, 1996. Т. 2. С. 162.

[5] *Духовской М. В.* Русский уголовный процесс. Москва, 1910. С. 205.

Народный Суд не стеснен формальными соображениями и от него зависит по обстоятельствам дела допустить те или иные доказательства, потребовать их от лиц, у которых они находятся. В этот период к доказательствам относились: заключения экспертов, показания свидетелей, вещественные доказательства, объяснения истца, ответчика[1].

В УПК РСФСР 1922 г. свобода оценки доказательств остается в числе правил доказывания, она производится по внутреннему убеждению, основанному на рассмотрении всех обстоятельств дела в их совокупности; установлено требование обоснования приговора проверенными в суде доказательствами; приведен перечень видов доказательств, решены другие вопросы **доказывания** по уголовным делам, не потерявшие своей актуальности и век спустя.

В 50-е гг. XX в. получила распространение «двойственная» концепция доказательств, разработанная М.С. Строговичем. Она явилась ответом на слабости понимания доказательств как фактов. В частности, доказательства, рассматриваемые исключительно как факты, по сути, сводила трактовку данного понятия исключительно к логическому доказыванию. Кроме того, факты как фрагменты реальной действительности к моменту производства по уголовному делу, осуществления доказывания существуют уже не всегда. Следовательно, факты как доказательства требуют интерпретации с позиций факта как знания, но в таком случае встает вопрос о том, с помощью каких средств приобретается это знание? Не отвечала концепция доказательств как фактов и на вопрос о том, что является доказательством, например в случае наличия прямых сведений о факте совершения преступления определенным лицом. Не может же факт быть доказательством самого себя?

«Двойственная» концепция доказательства получила классическое обоснование в работах М.С. Строговича; вместе с тем, ее основы просматривались уже в дореволюционной науке, в частности, в трудах Л.Е. Владимирова, который хотя и отмечал, что уголовным доказательством нужно считать всякий факт, имеющий назначением вызвать убеждение в существовании или несуществовании какого-либо обстоятельства, составляющего предмет судебного исследования[2], однако в указанной работе называл доказательствами также и показания обвиняемого, свидетелей и др.

Показания обвиняемого, свидетеля, заключения эксперта, документы, именуемые М.С. Строговичем источниками доказательств, признавались им доказательствами, поскольку содержали сведе-

---

[1] Собрание узаконений и распоряжений Рабочего и Крестьянского правительства. Москва, 1918. № 53. С. 597.

[2] *Владимиров Л.Е.* Учение об уголовных доказательствах. Тула: «Автограф», 2000. С. 133.

ния об отдельных фактах, с помощью которых устанавливались обстоятельства, подлежащие доказыванию. При такой конструкции понятия доказательств источники служили средством установления доказательств-фактов, а последние – средством установления обстоятельств, подлежащих доказыванию[1].

«Двойственное» понимание доказательств имело весьма прогрессивный для своего времени характер, поскольку включало понимание доказательств не только как фактов, но и как процессуальную форму сведений. Вместе с тем, эта концепция имела и слабости, поскольку не ставила задачей отказаться от понятия доказательств как фактов. Факты доказательствами быть не могут, поскольку, как явления реальной действительности, они не могут находится в уголовном деле, нередко их уже просто не существует. Если же считать фактом достоверное знание об определенных обстоятельствах, то это знание само должно основываться сведениях 2, как иначе могут быть доказаны факты? Оставалось неразрешенным и указанное выше противоречие в части определения прямых доказательств (факт не может быть доказательством самого себя). Вряд ли к факту применимо и такое понятие, как допустимость[3].

Доказательственные факты (факты, на основании которых делается логический вывод о наличии обстоятельств, подлежащих доказыванию) также становятся аргументом в логическом (отнюдь не информационном) доказывании лишь тогда, когда он установлен, поэтому, как справедливо подчеркивает П. А. Лупинская, доказательственные факты должны быть «установлены с соблюдением правил доказывания»[4]. В этой связи С. А. Шейфер отмечает, что существование материального объекта со следами преступления не превращает этот факт в доказательство, так как доказательством является не сам объект, а заключенная в нем либо в обстановке его обнаружения информация. Доказательственные факты – это знания о фактах реальной действительности[5], не сам фрагмент действительности.

Статья 69 УПК РСФСР 1960 г. определяла доказательства по уголовному делу как любые фактические данные, на основе кото-

---

[1] *Строгович М. С.* Избранные труды. Москва, 1991. Т. 3. С. 81–82.

[2] См. об этом подробнее: Курс советского уголовного процесса: Общая часть / под ред. А. Д. Бойкова и И. И. Карпеца. Москва, 1989. С. 555–562.

[3] *Орлов Ю. К.* Основы теории доказательств в уголовном процессе: научно-практическое пособие. Москва: Проспект, 2000. С. 36.

[4] *Лупинская П. А.* Доказательства и доказывание в новом уголовном процессе // Российская юстиция. 2002. № 7. С. 5–8.

[5] *Шейфер С. А.* Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования. Тольятти, 1998. С. 32.

рых в определенном законом порядке орган дознания, следователь и суд устанавливали наличие или отсутствие общественно опасного деяния, виновность лица, совершившего это деяние, и иные обстоятельства, имеющие значение для правильного разрешения дела[1].

УПК РФ в ч. 1 ст. 74 отказался от определения доказательств как «фактических данных», заменив его термином «сведения», что подчеркивает информационное содержание доказательства.

Замена термина «фактические данные» на «сведения» – оправданное решение. «Фактические данные» допускали неоднозначное толкование: и как сведения о фактах, и как сами факты (обстоятельства), значимые для уголовного судопроизводства[2]. Некоторые авторы полагали, что фактические данные – это цель, а доказательства – средства[3].

Одним из основоположников понимания доказательства как сведения о факте в середине 60-х гг. прошлого века стал В. Я. Дорохов, который выдвинул идею об «информационной модели» доказательства, которая состояла в том, что доказательство рассматривалось как единство сведений о фактах (информации) и их источника (материального носителя)[4]. Со временем «информационная модель» доказательств получила поддержку большинства ученых. Однако она, вне всякого сомнения, точно отражая сущность доказательства с процессуальной (правовой) точки зрения, не учитывает ту сторону познавательной деятельности в уголовном судопроизводстве, которая подчиняется логическим закономерностям. Такая сторона также существует. В той связи не все специалисты отказались рассматривать факты (доказательственные, т. е. промежуточные факты – аргументы в логическом доказывании) в качестве доказательств вместе со сведениями о фактах[5]. Другие авторы продолжают считать, что, наряду со сведениями о фактах и доказательственными фактами, те факты, которые устанавливаются должностными лицами, осуществляющими производство по уголовному делу в ходе отдельных следственных действий (например осмотра),

---

[1] Уголовно-процессуальный кодекс РСФСР: утв. ВС РСФСР 27.10.1960 (в ред. от 28.12.2001) // Рос. газ. 2001. 31 декабря.

[2] См., напр.: *Громов Н. А., Пономаренков В. А., Гущин А. Н., Францифоров Ю. В.* Доказательства, доказывание и использование результатов оперативно-розыскной деятельности. М., 2001. С. 72.

[3] *Францифоров Ю. В., Лубнин В. Н., Громов Н. А.* О дискуссионных вопросах в теории доказательств // Государство и право. 1998. № 5. С. 106.

[4] *Дорохов В. Я.* Понятие доказательства в советском уголовном процессе // Советское государство и право. 1964. № 9. С. 108–107.

[5] *Орлов Ю. К.* Структура судебного доказывания и понятие судебного доказательства // Вопросы борьбы с преступностью. Вып. 28. Москва, 1978. С. 86–101.

также представляют собой доказательства[1]. Подчеркнем, однако, что с правовой точки зрения доказательствами являются сведения о факте, которые должны обладать определенными свойствами (относимости и допустимости) и соответствовать предъявляемым законом требованиям (достоверности и в совокупности – достаточности). Факт же, как аргумент, в логическом доказывании или как знание о реальном обстоятельстве обладать свойством допустимости не может, равно как всегда априори должен считаться достоверным, между тем законодатель требует проверять достоверность доказательства (ст. 87 УПК РФ).

В современной науке распространено в целом верное представление, что в УПК РФ первая часть ст. 74 УПК РФ раскрывает содержание доказательства, а часть вторая данной нормы – его форму[2].

Однако в науке продолжают отстаиваться две точки зрения, разница между которыми не столь велика, как иногда представляется: а) доказательствами являются любые сведения; б) доказательство представляет собой единство фактических данных и их носителя – источника доказательств[3].

В известной работе Г. Ф. Горского, Л. Д. Кокорева и П. С. Элькинд по проблемам доказательств в советском уголовном процессе понятие доказательств толковалось как неразрывное единство содержания (фактических данных) и процессуальной формы (источников, в которых эти данные содержатся)[4]. Это, конечно, верно, однако вопрос возможности относительно самостоятельного рассмотрения процессуальной формы сведений и самих сведений стал краеугольным в дискуссии о понятии доказательства. Следствием этого вопроса является и разный подход к понятию «источник доказательств».

В УПК РФ не найти четкой позиции по вопросу о том, каким понятием охватываются различные виды процессуальной формы существования сведений о фактах (показания свидетеля, подозреваемого, обвиняемого, потерпевшего, эксперта, специалиста, заключение

---

[1] *Горский Г. Ф., Кокорев Л. Д., Элькинд П. С.* Проблемы доказательств в советском уголовном процессе. Воронеж: изд-во Воронеж. ун-та, 1978. С. 101.

[2] Более подробно см.: *Балашова А. А.* Научные подходы к понятию и признакам доказательств // Правовое регулирование общественных отношений на земле и в космическом пространстве: сборник материалов международной научно-практической молодежной конференции (9–10 ноября 2018 г.). Самара, 2018. С. 128–129.

[3] *Белкин А. Р.* Теория доказывания в уголовном судопроизводстве. Москва: Норма, 2005. С. 9–34.

[4] *Горский Г. Ф., Кокорев Л. Д., Элькинд П. С.* Проблемы доказательств в советском уголовном процессе. Воронеж: ВГУ, 1978.

эксперта, заключение специалиста, вещественные доказательства, протоколы следственных и судебных действий, иные документы). Эти категории именовались либо «источниками сведений о фактах»[1] (как составной части понятия доказательства), либо «источниками доказательств» (которые могли пониматься либо как неотъемлемая часть доказательств[2], либо как условно самостоятельная категория[3]). С точки зрения Л. Д. Кокорева и Н. П. Кузнецова, источником доказательств являются предметы материального мира, обладающие определенными свойствами, качествами и признаками и использующиеся для установления имеющих значение для дела обстоятельств, а также люди, в сознании которых запечатлелись эти обстоятельства[4].

П. А. Лупинская предлагала выделять материальные и процессуальные источники сведений о фактах. Процессуальные источники – процессуальная форма сведений, материальные – люди, предметы[5]. Мысль П. А. Лупинской представляется логичной. Однако материальные источники – категория непроцессуальная и может использоваться в научных трудах для объяснения процессуальных категорий с использованием диалектического метода. Эта категория позволяет понять, каким образом формируется доказательство, а не что такое само доказательство. Соотношение процессуального источника сведений о фактах как процессуальной формы сведений о них с источником доказательства остается дискуссионным.

Полагаем, проблема несколько преувеличена. Вряд ли специалисты решатся отрицать, что сведение является доказательством только в том случае, если существует в определенной процессуальной форме. Собственно именно процессуальной формой и определяется допустимость доказательства как его неотъемлемое свойство. Сторонники понимания доказательства как единства содержания и формы считают, что сведения должны признаваться только содержанием уголовно-процессуальных доказательств, но не самими доказательствами по уголовному делу[6]. Однако

---

[1] См., напр.: *Кокорев Л. Д., Кузнецов Н.П.* Уголовный процесс: доказательства и доказывание. Воронеж, 1995. С. 113.

[2] См., напр.: *Бедняков Д. И.* Непроцессуальная информация и расследование преступлений. Москва, 1991. С. 57.

[3] *Чельцов М. А.* Советский уголовный процесс. Москва, 1962. С. 132 и далее.

[4] *Кокорев Л. Д., Кузнецов Н. П.* Уголовный процесс: доказательства и доказывание. Воронеж, 1995. С. 114–115.

[5] Уголовно-процессуальное право Российской Федерации: учебник / отв ред. П. А. Лупинская. Москва, 2003. С. 228.

[6] *Костенко Р.В.* Понятие и признаки уголовно-процессуальных доказательств. Москва: Юрлитинформ, 2006. С. 19.

Л. М. Карнеева, например, верно отмечала, что неразрывная связь между доказательством и его формой не мешает их условно разграничивать в целях получения в доказывании правильного результата. Действительно, сведения об одном факте могут быть получены из нескольких источников, равно из одного источника могут быть получены сведения о нескольких фактах[1]. О том же пишут и другие авторы[2]. В этой связи именовать процессуальную форму сведений о фактах источниками доказательств вполне допустимо, не ставя при этом под сомнение невозможность существования доказательства вне процессуальной формы сведения о факте («источник доказательства» – в данном случае специальный термин, означающий процессуальную форму сведения о факте). При этом понимание источника доказательств как процессуальной формы сведения о факте не будет полным, если не учитывать конкретного субъекта, представившего информацию, иначе одни и те же сведения, полученные от разных лиц, должны признаваться одним и тем же доказательством, поскольку имеют одинаковую процессуальную форму. Конечно, это был бы нонсенс[3].

Итак, сведения об обстоятельствах, подлежащих доказыванию, являются доказательствами, только если существуют в определенной процессуальной форме (в форме источников доказательств). Заметим, что в легальном определении доказательств (ч. 1 ст. 74 УПК РФ) не учитывается такое их свойство, как допустимость. Законодатель не указывает на то, что сведения, являющиеся доказательствами, сами должны быть получены с соблюдением процессуальной формы. В определение доказательства желательно было бы заложить его неотъемлемое свойство – допустимость. После этого взгляды на доказательство как на сведение, не требующее соблюдение при получении процессуальной формы, станут еще более спорными. Так, например, существует подход, согласно которому процессуальная форма собирания доказательств ставит стороны в неравные условия, само доказательство представляет собой объективно существующую информацию, а вовсе не результат познава-

[1] *Карнеева Л. М.* Доказательства и доказывание в уголовном процессе: учебное пособие. Москва: УМЦ при ГУК МВД РФ, 1994. С. 9.

[2] *Фаткуллин Ф. Н.* Общие проблемы процессуального доказывания. Казань, 1976. С. 110–112; *Орлов Ю. К.* Основы теории доказательств в уголовном процессе: научно-практическое пособие. Москва.: Проспект, 2000. С. 39.

[3] *Фаткуллин Ф. Н.* Общие проблемы процессуального доказывания. Казань, 1976. С. 127.

тельной деятельности следователя[1]. Допустимость доказательства, т. е. соблюдение при получении сведения процессуальной формы – важная гарантия не только правильного познания, но и соблюдения прав человека, в том числе и участников судопроизводства, представляющих строну защиты. Иначе неизбежно произойдет игнорирование процедуры в целом, а уголовное судопроизводство сольется с иными видами познания (обыденное, оперативно-розыскное и т. д.), не обладающими необходимыми гарантиями качества познавательного результата, позволяющими обосновывать им процессуальные решения[2].

Доказательства – сведения, то есть информация, воспринимаемая и перерабатываемая людьми. Доказательственная информация – сведения, которые обладают свойствами относимости и допустимости. Можно говорить о том, что доказательства и доказательственная информация – синонимы[3]. Категорически нельзя согласиться, что существует разница между понятиями «собирание доказательств» и «собирание доказательственной информации». Специалисты, считающие, что собирание доказательственной информации может осуществляться и непроцессуальными путями[4], не учитывают, что ведут речь лишь о потенциально доказательственной информации, а не о собственно доказательственной.

Рассматривая отдельные виды доказательств, перечисленные в ч. 2 ст.74 УПК РФ, следует отразить возможность и особенности их формирования на электронных носителях информации.

---

[1] *Лазарева В. А.* Доказывание в уголовном процессе: учебно-практич. пособие. Москва: Высшее образование, 2009. С. 57–62.

[2] *Победкин А. В., Яшин В. Н.* Следственные действия. Москва: Юрлитинформ, 2016. С. 11.

[3] *Кокорев Л. Д., Кузнецов Н. П.* Указ. раб. С. 116–117.

[4] *Алиев Т. Т., Громов Н. А., Макаров Л. В.* Уголовно-процессуальное доказывание. Москва, 2002. С. 7. Существует мнение, что некоторым результатам оперативно-розыскной деятельности следует придать доказательственное значение. См., напр.: *Россинский С. Б.* Результаты оперативно-розыскной деятельности – доказательства по уголовному делу: только «за» и «никаких» против // Деятельность правоохранительных органов в современных условиях: сборник материалов XXIII Международной научно-практической конференции (24 –25 мая 2018 г., Восточно-Сибирский институт МВД России): в 2-х т. Иркутск: Восточно-Сибирский институт МВД России. 2018. С. 265–271. Однако российский уголовный процесс построен на безусловном приоритете уголовно-процессуальной формы, которая является действенной гарантией правильного результата и обеспечения прав личности. Результаты оперативно-розыскной деятельности на легальных основаниях без серьезных проблем могут быть представлены следователю, дознавателю и в суд и использованы в уголовно-процессуальном доказывании в порядке, регламентирующем собирание, проверку и оценку доказательств. См.: Об Оперативно-розыскной деятельности: федеральный закон от 12 августа 1995 г. № 144- ФЗ // Собр. законодательства Рос. Федерации. 1995. № 33. Ст. 3349.

1. Показания подозреваемого, обвиняемого, потерпевшего, свидетеля, эксперта. В соответствии со ст. 76–80 УПК РФ показания – это сведения, сообщенные указанными выше лицами на допросе, проведенном в ходе досудебного производства. Надо полагать, что показания могут быть получены и в ходе производства очной ставки.

Традиционно основным процессуальным средством фиксации доказательственной информации в процессе допроса является протокол, требования к форме и содержанию которого представлены в ст. 166 УПК РФ с конкретизацией в ст. 174 и ст. 190 УПК РФ. В качестве дополнительного средства фиксации зачастую применяется аудио- или видеозапись. Использование аудио- и видеозаписи повышает полноту и точность фиксации показаний, а также передает эмоциональную сторону показаний. Учитывая, что современные средства аудио- и видеозаписи являются цифровыми, в результате их применения создается файл данных, который обладает всеми свойствами компьютерной (цифровой) информации, рассмотренными в предыдущих параграфах.

В соответствии с требованиями п. 8 ст. 166 УПК РФ электронный носитель, содержащий файлы аудио- и видеозаписи допроса, является приложением к протоколу допроса. Согласно ч. 4 ст. 190 УПК РФ в протоколе допроса отражаются сведения о технических средствах, об условиях аудио- и (или) видеозаписи, факте приостановления аудио- и (или) видеозаписи, о причине и длительности остановки их записи и заявления допрашиваемого лица по поводу проведения аудио- и (или) видеозаписи. По окончании получения показаний файл с записью в присутствии участников допроса целесообразно скопировать на неперезаписываемый электронный носитель, например CD-R-диск, отразив в протоколе используемое программное обеспечение, серийный номер носителя, имя, размер, дату и время создания файла[5].

Нельзя не заметить, что относительно процессуального статуса приложений к протоколу следственного действия ведется острая дискуссия. Действительно, «приложение к протоколу» отнюдь не означает, что результаты применения технических средств фиксации являются частью протокола. Если бы это было так, то информация, содержащаяся в результатах применения технических средств фиксации,

[5] *Гаврилин Ю.В.* Организационно-методическое обеспечение расследования преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации // Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: в 2 ч. Москва: Академия управления МВД России, 2019. Ч. 1. С. 128–129.

но отсутствующая в протоколе, не имела бы никакого доказательственного значения. Между тем, очень давно А.А. Леви справедливо заметил, что поскольку необходимая информация может иногда содержаться не в протоколе, а в материалах звукозаписи, именно ее содержание может стать основой процессуального решения[1], хотя он и не вышел за представление о звукозаписи как о составной части протокола.

Полагаем, самостоятельное доказательственное значение информации, содержащейся в приложениях к протоколу, может признаваться, если только такие приложения не ограничивать неясным процессуальным статусом, а прямо признать, что они представляют собой иной документ, что, в свою очередь, не исключает рассмотрения их как приложений к протоколу следственного действия.

Кроме того, протоколирование и применение технических средств фиксации – различные физические средства фиксации информации. В первом случае это письменная вербальная информация. Во втором – или наглядно-образная, или устная вербальная. Очевидно, что такая форма фиксации информации не может обеспечить результат, считающийся частью протокола, то есть частью письменной вербальной информации. Каждый источник доказательств предполагает фиксацию строго определенным способом информацию определенной физической формы. Разные способы фиксации предполагают формирование различных источников доказательств. Следовательно, результаты применения технических средств фиксации не формируют показания.

Представляется, что приложения к протоколу следственного действия полностью подпадают под понятие иного документа. Иные документы вовсе необязательно формируются вне уголовного процесса, как иногда полагают[2]. Иные документы могут формироваться и за рамками судопроизводства, и в его ходе[3] (объяснение, протокол явки с повинной и др.).

Н.П. Кузнецов решал вопрос о статусе результатов технических средств фиксации дифференцированно. Он полагал, что фонограмма допроса – приложение к протоколу, а планы и схемы, составленные в ходе следственного действия, – либо самостоятельный источник доказательств, либо часть протокола[4]. Основания предложенной дифференциации здесь недостаточно ясны. Приложением к протоколу являются

---

[1] *Леви А.А.* Звукозапись в уголовном процессе. Москва, 1974. С. 11–12.

[2] *Копьева А.Н.* Указ. раб. С. 6; *Строгович М.С.* Курс советского уголовного процесса. Т. 1. С. 458–459.

[3] См., напр.: *Кокорев Л.Д., Кузнецов Н.П.* Указ. раб. С. 213.

[4] *Кокорев Л.Д., Кузнецов Н.П.* Указ. раб. С. 139–140.

и те и другие результаты, однако это не лишает их статуса иных документов. Планы, схемы, аудиозапись – отнюдь не письменная вербальная информация, характерная для протокола. Следовательно, их доказательственное значение – значение не показаний, а иных документов.

Не стоит опасаться, что при таком понимании процессуального статуса приложений к протоколам следственного действия последние сами станут приложением к результатам применения технических средств[1]. Уголовному судопроизводству известны ситуации, когда допустимость одного источника доказательств определяется существованием другого (протокол осмотра вещественного доказательства – самостоятельный источник доказательства, равно как и само вещественное доказательство; показания эксперта могут быть допустимым доказательством лишь в случае предварительного получения заключения эксперта и др.). В рассматриваемом случае протокол следственного действия является условием допустимости приложения к нему – иного документа, который, в свою очередь, формируется по установленным для данного источника доказательства правилам.

Учитывая, что использование технологии видео-конференц-связи для производства допроса предусмотрено лишь для судебных стадий уголовного процесса (ч. 6.1 ст. 240, ст. 278.1, ч. 8 ст. 389.13 УПК РФ), представляют интерес предложения, направленные на дополнение УПК РФ нормой, предусматривающей особенности допроса свидетеля по уголовному делу посредством видео-конференц-связи[2]. Целесообразность уголовно-процессуальной регламентации порядка производства следственных действий, участники которых территориально находятся в разных местах, отмечали и авторы настоящего пособия[3], при условии соблюдения следующих технических условий: устойчивость канала связи в режиме телеконференции; возможность преобразование устной речи в письменный текст; возможность ознакомления участников следственного действия с протоколом в режиме online; удостоверение протокола с использованием технологий биометрической идентификации и электронной подписи.

---

[1] *Семенцов В. А.* Видео- и звукозапись в доказательственной деятельности следователя: дис. ... канд. юрид. наук. Екатеринбург, 1994. С. 57.

[2] *Антонович Е. К.* Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств) // Актуальные проблемы российского права. 2019. № 6 (103). С. 128.

[3] *Гаврилин Ю. В.* Трансформация уголовно-процессуальной формы в условиях цифровой экономики // Уголовный процесс и криминалистика: теория, практика, дидактика: сборник статей IV Всероссийской науч.-практ. конф. / под ред. А. В. Красильникова. Москва: Академия управления МВД России, 2019. С. 118.

Кроме того, целесообразны дополнительные гарантии, обеспечивающие возможность реализации допрашиваемым прав в полном объеме.

Таким образом, в процессе получения показаний и их фиксации с применением цифровой аудио-, видеозаписи формируются доказательства на электронном носителе информации, выступающие в виде приложения к протоколу следственного действия.

2. Протоколы следственных и судебных действий. Чаще всего фото-, видео- или аудиофиксация с использованием цифровых электронных носителей информации используется в качестве дополнительного средства фиксации при производстве осмотра места происшествия, обыска, выемки, проверки показаний на месте, следственного эксперимента, а также допросов, о чем было сказано выше.

3. Вещественные доказательства. Согласно ст. 81 УПК РФ вещественные доказательства – это любые предметы: которые служили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления; на которые были направлены преступные действия; деньги, ценности и иное имущество, полученные в результате совершения преступления; иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

Особую группу вещественных доказательств в силу свойственной им определенной электронной специфики составляют электронные носители информации[1].

Анализ изученных нами уголовных дел показал, что при изъятии электронных носителей информации в 93 % случаев они признавались вещественными доказательствами и лишь в 7 % – иными документами. Заметим, что в ряде случаев по содержанию электронные носители представляли собой именно иные документы, хотя оформлялись как вещественные доказательства, поскольку оптимальной процессуальной формы признания электронных носителей информации иными документами в УПК РФ не содержится.

4. Иные документы. Согласно ст. 84 УПК РФ иные документы допускаются в качестве доказательств, если изложенные в них сведения имеют значение для установления обстоятельств, входящих в предмет доказывания.

Именно «иные документы», по мнению А.Р. Белкина, придают системе доказательств полноту и завершенность, позволяя, наряду с другими доказательствами, вовлекать в уголовные дела любую

[1] *Краснова Л.Б.* Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Серия: Экономические и юридические науки. 2013. № 4. С. 255.

информацию, имеющую доказательственное значение[1]. Это было бы, несомненно, так, если бы порядок приобщения к уголовному делу иных документов различной физической формы был бы предусмотрен в УПК РФ. Однако ст. 84 УПК РФ не предусматривает процессуальной формы приобщения к уголовному делу «иных документов».

Согласно ч. 2 ст. 84 УПК РФ документы могут быть зафиксированы на различных носителях, включая фото-, кино-, аудио-, видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, установленном ст. 86 УПК РФ (обратим внимание, что и эта статья не предусматривает порядка «получения, истребования или представления», а устанавливает, что компетентные должностные лица собирают доказательства путем производства следственных или иных процессуальных действий). Разнообразие носителей иных документов как источников доказательств достаточно давно признано и в науке уголовного процесса. Так, Д.Б. Игнатьев справедливо указывал: «...иные документы могут содержать сведения, зафиксированные как в письменной, так и в иной форме: в виде фото- и киносъемки, звуко- и видеозаписи, кодов, шифров, электронных документов, автоматической самозаписи и других носителей информации, фиксируемой с помощью всевозможных научно-технических средств»[2].

Развитие цифровых технологий актуализировало вопрос о месте документов на электронных носителях информации в системе источников доказательств. При этом следует подчеркнуть, что если доказательственное значение имеет исключительно содержание документированной информации, находящейся на электронном носителе, то она, а точнее ее носитель, в соответствии с положениями ст. 84 УПК РФ, относится к иным документам. Вещественные доказательства отличаются от иных документов не внешними характеристиками, которые могут быть абсолютно одинаковыми, а содержательными признаками[3].

Электронные носители недокументированной информации, а также документированной информации, несущей на себе следы преступления (например модификации компьютерной информации) или отвечающие иным признакам, указанным в ст. 81 УПК РФ, относятся к вещественным доказательствам.

---

[1] *Белкин А.Р.* Новеллы уголовно-процессуального законодательства – шаги вперед или возврат на проверенные позиции? // Уголовное судопроизводство. 2013. № 3. С. 4–13.

[2] *Игнатьев Д.Б.* Документы как доказательства по делам о налоговых преступлениях: автореф. дис. ... канд. юрид. наук. Волгоград, 2001. С. 13.

[3] *Победкин А. В.* Уголовно-процессуальное доказывание. Москва: Юрлитинформ, 2009. С. 143.

Не всегда для того, чтобы считаться иным документом, электронный носитель информации должен содержать предусмотренные нормами права реквизиты или согласованные существенные условия его применения: порядок составления, способы проверки и другие, как полагает, например, А.В. Ткачев[1]. Все иные характеристики информации на электронном носителе, кроме предусмотренных ст. 81 УПК РФ, свидетельствуют, что мы имеем дело с иным документом.

Результаты проведенного социологического исследования свидетельствуют о явно нереализованной потребности в использовании рассматриваемой процессуальной формы. В этой связи ранее авторами настоящего пособия предлагалось решить на законодательном уровне вопрос о порядке признания носителей информации (включая и электронные носители) «иными документами», порядок их хранения, возвращения законным владельцам и т. д.[2] В своей более поздней совместной работе авторами указывалось, что документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием информационно-телекоммуникационной сети Интернет, а также документы, подписанные электронной подписью в порядке, установленном законодательством Российской Федерации, необходимо допустить в качестве доказательств[3].

В настоящее время, действительно, объекты физической формы, не совпадающие с формой листа формата, соответствующего листам уголовного дела, не могут быть просто к нему приложены. В материалах уголовного дела должны быть сведения о том, что такой объект находится при уголовном деле, а также описаны его характерные признаки и содержание. Иначе говоря, необходим осмотр документа, составление протокола его осмотра, вынесение постановления о приобщении предмета к уголовному делу. Именно таким образом к уголовному делу приобщаются вещественные доказательства, и такой порядок распространяется на электронные носители информации.

Рассматривая вопрос о месте электронных носителей информации в системе доказательств, следует затронуть еще один вопрос. В условиях бурной цифровизации и все большего распространения

---

[1] *Ткачев А.В.* Вопросы использования электронных носителей компьютерной информации в уголовном процессе в качестве доказательств иных документов // Известия Тульского государственного университета. Серия: Экономические и юридические науки. 2016. № 3–2. С. 440.

[2] *Гаврилин Ю.В., Победкин А.В.* Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы // Труды Академии управления МВД России. 2018. № 3 (47). С. 112.

[3] *Гаврилин Ю. В., Победкин А.В.* Модернизация уголовно-процессуальной формы в условиях информационного общества // Труды Академии управления МВД России. 2019. № 3 (51). С. 35.

преступлений, совершенных с использованием информационно-телекоммуникационных технологий, для которых характерны так называемые цифровые следы[1], в научной литературе на протяжении ряда лет ведется активная дискуссия относительно необходимости введения в уголовный процесс так называемых «электронных доказательств» в качестве самостоятельного вида доказательств[2]. В частности, с указанной целью предлагается дополнить ст. 74 УПК РФ понятием «электронное доказательство», или «цифровое доказательство».

В. Н. Григорьев и О. А. Максимов полагают целесообразным выделить электронные носители информации в отдельный вид (источник) доказательства и определить его как «предмет, содержащий значимую для уголовного дела информацию, созданную не в процессе расследования (раскрытия) уголовного дела, восприятие которой невозможно без использования электронно-вычислительных средств»[3].

Н. А. Зигура сведения о фактах, существующие в электронно-цифровой форме, также предлагает рассматривать как самостоятельный вид доказательств[4].

Р. И. Оконенко под «электронным доказательством» предлагает понимать электронный носитель информации, содержащий сведения о значимых обстоятельствах по конкретному уголовному делу и обладающий следующими юридически значимыми признаками:

а) значительным объемом памяти;

б) простотой передачи и копирования сведений с одного электронного носителя информации на другой;

в) возможностью удаленного доступа к содержанию электронного носителя и информационно-телекоммуникационным системам (в частности к сети Интернет);

г) относительностью и неочевидностью содержания[5].

---

[1] *Россинская Е. Р.* Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина. 2019. №. 5 (57). С. 31–44.

[2] Более подробно см.: *Балашова А. А.* Соотношение понятий «вещественное доказательство» и «электронное доказательство» // Уголовный процесс и криминалистика: теория, практика, дидактика (современные проблемы досудебного производства: уголовно-процессуальные, криминалистические и организационные аспекты): сборник материалов V Всероссийской науч.-практ. конф. (6 декабря 2019 г.). Рязань, 2019. С. 36–43.

[3] *Григорьев В. Н., Максимов О. А.* Некоторые вопросы использования электронных носителей информации при расследовании уголовных дел // Полицейская деятельность. 2018. № 1. С. 1–8. DOI: 10.7256/2454-0692.2018.1.26103. URL: https://nbpublish.com/ library_read_article.php?id=26103 (дата обращения: 01.03.2020).

[4] *Зигура Н. А.* Компьютерная информация как вид доказательств в уголовном процессе России: дис. ... канд. юрид. наук. Челябинск, 2010. С. 210.

[5] *Оконенко Р. И.* Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы рос-

По мнению С. П. Ворожбит, электронные средства доказывания охватываются всеми известными видами доказательств, но нуждаются в дополнительной процессуальной регламентации[1].

Одновременно в научной литературе обширно представлена и иная точка зрения. Так, Н. А. Иванов, отмечая условный характер терминологии «компьютерные», «электронные» или «цифровые доказательства», полагает, что они не являются особым или отдельным видом доказательств [2].

В свою очередь Н. В. Олиндер[3] высказывает мнение, что термин «электронное доказательство» является некорректным, правильным будет название «цифровое доказательство». Далее автор делает вывод о том, что доказательства, содержащие цифровую информацию, – это вещественные доказательства, которые представлены в виде документов, имеющих цифровую форму и которые облечены в материальную форму с помощью специальных аппаратных средств и программных продуктов (распечатаны на принтере, скопированы на носитель цифровой информации и т. д.).

По мнению П. С. Пастухова, электронное доказательство – это электронная информация, полученная субъектом доказывания способом, прямо не запрещенным законом, и представленная в суд в установленном законом порядке, способная обеспечить правильное разрешение уголовного дела по существу[4]. При этом автор полагает, что механизмы образования «обычного» вещественного доказательства и электронного доказательства различны и вопрос о процессуальной форме электронного доказательства является неоднозначным. Дискуссионность его вызвана тем, что в теории неоднозначно трактуется само понятие вещественного доказательства. Однако и он придерживается мнения, что нет необходимости выделять новый вид «электронных доказательств».

сийского права. 2015. № 3 (52). С. 120.

[1] *Ворожбит С. П.* Электронные средства доказывания в гражданском и арбитражном процессе: автореф. дис. ... канд. юрид. наук: 12.00.05. Санкт-Петербург, 2011. С. 2.

[2] *Иванов Н. А.* Цифровая информация в уголовном процессе // Библиотека криминалиста. 2013. № 5 (10). С.100.

[3] *Олиндер Н. В.* К вопросу о доказательствах, содержащих цифровую информацию // Юридический вестник Самарского университета. 2017. № 3. С.107.

[4] *Пастухов П. С., Терехин В. В.* К вопросу о понятии и сущности электронных доказательств в уголовном процессе // Вестник КРАГСиУ. Серия: Государство и право. 2014. № 18. С. 71.; *Балашова А. А.* Соотношение понятий «вещественное доказательство» и «электронное доказательство» // Уголовный процесс и криминалистика: теория, практика, дидактика (современные проблемы досудебного производства: уголовно-процессуальные, криминалистические и организационные аспекты): сборник материалов V Всероссийской научно-практической конференции (6 декабря 2019 г.). Рязань, 2019. С. 36–43.

Аналогичную точку зрения высказывает и К. Б. Калиновский, считая, что электронные доказательства – это данные, относимые к делу точно так же, как и любые другие процессуальные данные, которые свободно могут использоваться в качестве ориентирующей, тактической информации[1]. Иными словами, электронные доказательства не являются отдельным видом доказательств.

Практически такую же позицию занимает и С. В. Зуев, который считает, что, несмотря на существенные особенности, электронная информация вполне может быть представлена в виде одного из традиционных доказательств – вещественного доказательства или иного документа[2].

Полагаем, что с учетом наличия в действующем законодательстве специальных правил по работе с электронными носителями информации, предложение о введении понятия «электронное доказательство» не целесообразно, поскольку оно будет дублировать положения о работе с электронными носителями информации. Существующие процессуальные формы позволяют использовать информацию на электронных носителях информации и в качестве вещественного доказательства, или в качестве иного документа.

Доказательственное значение иного документа в электронной форме, как и электронного носителя информации – вещественного доказательства, определяется, прежде всего, содержащейся в нем информацией. Однако в отличие от электронного носителя информации – вещественного доказательства информация, содержащаяся в ином документе в электронной форме, не связана с конкретным материальным объектом-носителем и при утрате носителя может быть восстановлена, а главное – не обладает признаками, предусмотренными ст. 81 УПК РФ: не служила средством совершения преступления, не несет на себе его следы, не являлась предметом преступного посягательства, не была получена в результате совершения преступления, не может служить средством для обнаружения преступления и установления обстоятельств уголовного дела.

Принимая во внимание изложенное, представляется целесообразным дополнить ч. 2 ст. 84 УПК РФ «Иные документы» положениями, содержащими порядок приобщения к уголовному делу и хранения

---

[1] *Калиновский К. Б., Маркелова Т. Ю.* Доказательственное значение «электронной» информации в российском уголовном процессе // Российский следователь. 2001. № 6. С. 18–19.

[2] Зуев С. В. Электронные доказательства, используемые в уголовном процессе // Международная Ассоциация Содействия Правосудию: сайт. URL: https://www.iuaj.net/node/2666 (дата обращения: 24.12.2019).

электронных носителей информации, которые по содержанию являются не вещественными доказательствами, а иными документами.

В завершении параграфа представляется необходимым указать следующие выводы:

1. Имеющиеся недостатки в уголовно-процессуальной регламентации работы с доказательствами на цифровом носителе сами по себе не являются основанием для введения в уголовно-процессуальный закон новой процессуальной формы цифровых доказательств, поскольку их получение возможно в рамках существующих процессуальных форм.

2. В отличие от электронного носителя информации – вещественного доказательства информация, содержащаяся в ином документе в электронной форме, не связана с конкретным материальным объектом-носителем и не обладает признаками, предусмотренными ст. 81 УПК РФ.

3. Существует необходимость процессуальной регламентации порядка приобщения к уголовному делу и хранения электронных носителей информации, содержащих доказательства в форме иных документов.

Вопросы для повторения

1. Понятие и свойства доказательств.
2. Соотношение доказательств и их источников.
3. Свойства доказательств.
4. Классификация доказательств.
5. Содержание научной дискуссии о введении в закон «цифровых доказательств».
6. Проблема использования электронных носителей информации в качестве «иного документа».

Практическое задание

Определить, к какому виду доказательств относятся следующие объекты:

– электронный носитель, содержащий файлы аудио-, видеозаписи допроса;

– ответ из Росреестра о наличии в собственности обвиняемого недвижимого имущества, поступивший в форме электронного документа;

– видеозапись с камеры видеорегистратора автомобиля, запечатлевшая момент ДТП.

§ 3. Современное состояние и проблемы использования информации, содержащейся на электронных носителях, в процессе доказывания

Развитие информационно-телекоммуникационных технологий и их активное использование в повседневной жизни открыли новые возможности для обмена информационными ресурсами между их пользователями. Одновременно с этим возникла потребность правового регулирования вопросов правомерного получения информации, содержащейся на электронных носителях, в рамках процедур, предусмотренных уголовно-процессуальным законодательством.

Как уже ранее отмечалось, правовая категория «электронный носитель информации» была введена в уголовно-процессуальное законодательство Федеральным законом от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» с целью упорядочения и конкретизации процедуры их изъятия в ходе расследования, а также решения вопросов о порядке их возвращения и (или) копирования содержащейся на них информации. Кроме того, ставилась задача дополнительной защиты прав субъектов предпринимательской деятельности и обеспечение возможности продолжения их функционирования в случае изъятия электронных носителей[1].

В результате в ст. 81, 82, 166, 182 и 183 УПК РФ были внесены значительные изменения, предоставляющие законному владельцу информации права на получение копии данных, содержащихся на электронном носителе, изымаемом в ходе следственного действия. В частности, ч. 2.1 ст. 82 УПК РФ «Хранение вещественных доказательств» была дополнена указанием на то, что после производства неотложных следственных действий в случае, если были изъяты электронные носители информации и отсутствовала возможность их возврата законному владельцу, то содержащаяся на этих носителях информация по ходатайству их законного владельца может быть скопирована.

Пункт 5 ч. 2 указанной нормы дополнен положением о том, что электронные носители информации должны храниться в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации,

[1] Пояснительная записка «К проекту Федерального закона «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Доступ из справ.-правовой системы «КонсультантПлюс».

и если это возможно без ущерба для доказывания, то они возвращаются их законному владельцу после осмотра и производства других необходимых следственных действий.

Статья 166 УПК РФ была дополнена ч. 8, устанавливающей, что к протоколу прилагаются электронные носители информации, полученной или скопированной с других электронных носителей информации в ходе производства следственного действия[1].

Весьма существенными новеллами в процессуальном порядке работы с электронными носителями информации стали дополнения ст. 182 и ст. 183 УПК РФ соответственно частями 9.1 и 3.1, устанавливающими процессуальные требования к порядку изъятия электронных носителей информации в ходе производства обыска и выемки. Вводилось требование об обязательном участии специалиста при изъятии электронных носителей, а также право законного владельца изымаемых электронных носителей заявлять ходатайство о копировании информации, содержащейся на электронных носителях[2].

Учитывая, что терминологический аппарат, использованный в конструкциях рассматриваемых процессуальных норм, был введен в общие правила производства обыска и выемки, данные новеллы затронули всю процессуальную деятельность органов предварительного расследования, осуществляемую не только по экономическим преступлениям, но и по всем тем уголовным делам, в предмет доказывания которых входят обстоятельства, свидетельствующие об использовании «электронных носителей информации» подозреваемым (обвиняемым) в ходе подготовки, совершения, сокрытия преступления.

Заметим, что приведенные положения не в полной мере смогли разрешить существовавшие в следственной практике проблемные вопросы[3]. Об этом также свидетельствуют многочисленные апелляционные и кассационные жалобы адвокатов по уголовным делам и неоднозначная практика принятия судебных решений. В связи с этим дальнейшее развитие процессуальной регламентации собирания доказательственной информации на электронных носителях развивалось по следующим направлениям.

Федеральным законом от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» формулировка ч. 2.1

---

[1] Собственно, ничего нового к общему порядку приобщения к протоколу следственного действия изъятых (скопированных) материалов указанная норма не добавила.

[2] В настоящее время утратили силу.

[3] *Зуев С. В.* Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С. 58.

ст. 82 «Хранение вещественных доказательств» претерпела изменения, а именно текст «может быть скопирована» применительно к информации, находящейся на электронных носителях, был заменен на текст «копируется» в виде категоричного императивного предписания. Представляется, что предложенная законодателем новая формулировка «копируется» является более конкретной по сравнению с предыдущей формулировкой «может быть скопирована», поскольку сокращает пределы произвольного усмотрения должностных лиц со стороны обвинения при решении вопроса о производстве копирования или отказа от копирования. Не вызывает сомнений, что при копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения[1].

Дальнейшее развитие уголовно-процессуального законодательства в части регламентации порядка изъятия электронных носителей информации связано с принятием Федерального закона от 03.07.2016 № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности», которым ограничены сроки признания вещественными доказательствами электронных носителей информации, изъятых в ходе досудебного производства по уголовным делам об отдельных видах преступлений экономической направленности, совершенных в сфере предпринимательской деятельности. Кроме того, предусмотрен конкретный срок возврата законному владельцу электронных носителей, не признанных вещественными доказательствами.

Как подчеркивается в постановлении Пленума Верховного Суда Российской Федерации от 15.11.2016 № 48 «О практике применения судами законодательства, регламентирующего особенности уголовной ответственности за преступления в сфере предпринимательской и иной экономической деятельности»[2], успешное достижение стоящих перед бизнес-сообществом целей во многом зависит от наличия действенных организационно-правовых механизмов, позволяющих исключить возможность использования уго-

---

[1] *Старичков М.В.* Использование информации из компьютерных сетей в качестве доказательств // Право и кибербезопасность. 2014. № 2. С. 43.

[2] О практике применения судами законодательства, регламентирующего особенности уголовной ответственности за преступления в сфере предпринимательской и иной экономической деятельности: постановление Пленума Верховного Суда Российской Федерации от 15 ноября 2016 г. № 48 // Бюллетень Верховного Суда Российской Федерации. 2017. № 1 (далее – Верховный Суд).

ловного преследования в качестве средства давления на предпринимательские структуры.

Существует мнение, что такое давление вызывается тем, что предпринимательская деятельность зачастую влечет вынужденное (умышленное или неосторожное) совершение ее субъектами правонарушений, что создает «питательную среду» для разного рода злоупотреблений со стороны отдельных представителей правоохранительных и контролирующих органов, принуждая внешне законными, равно как и противоправными, методами к коррупционным проявлениям[1]. Приведенные обстоятельства и послужили основанием для принятия рассматриваемых норм уголовно-процессуального закона.

Справедливости ради обозначим, что статистические данные, приведенные в специальных исследованиях, не подтверждают, что правоохранительные структуры массово «давят» на бизнес-сообщество в целях получения незаконных выгод[2]. В этой связи изменения в уголовно-процессуальный закон по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности вызывают разное отношение специалистов.

В любом случае совершенствование УПК в части установления особенностей порядка производства по указанной категории уголовных дел, включая изъятие электронных носителей информации, должны позволять устанавливать обстоятельства по уголовному делу полно и правильно. Все особенности производства, устанавливая дополнительные гарантии экономической безопасности государства, не должны препятствовать уголовно-процессуальному доказыванию, поскольку вред экономической безопасности преступностью в сфере предпринимательской деятельности может быть не меньшим, чем от преступной деятельности отдельных представителей правоохранительных структур[3].

Федеральным законом от 06.07.2016 № 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» ст. 185 УПК РФ была дополнена ч. 7, согласно которой если имеются достаточные основания

---

[1] *Бажанов С.В.* Состояние законности при возбуждении уголовных дел и расследовании преступлений, совершаемых предпринимателями // Право и экономика. 2017. № 8. С. 17–25.

[2] *Панфилов П.О.* Особенности производства по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности: автореф. дис. ... канд. юрид. наук. Москва, 2019. С. 16.

[3] *Панфилов П.О.* Указ раб. С. 7–8 и др.

полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка[1].

Федеральным законом от 27.12.2018 № 533-ФЗ «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» положения ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ, связанные с порядком изъятия электронных носителей и копирования информации, утратили силу. При этом законодателем сформулированы универсальные требования к порядку собирания доказательств на электронных носителях в специально введенной ст. 164.1. «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий». Следует заметить, что незадолго до приведенных изменений подобные предложения уже были сформулированы авторами настоящего пособия, предложившими признать утратившими силу положения ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ, с одновременным введением общей нормы, регламентирующей процессуальный порядок и особенности обнаружения, фиксации изъятия доказательственной информации на электронных носителях в ходе следственных действий[2].

Сравнительный анализ утративших силу положений, затрагивающих проведение обыска и выемки в части изъятия электронных носителей информации, и вновь введенных положений позволяет констатировать следующее:

1. Законодателем определено копирование информации в качестве приоритетного способа собирания доказательств на электронных носителях по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности. Вероятно, при этом законодателем положительно воспринято ранее отраженное в научной литературе соответствующее предложение[3], а также учтены интересы предпринимателей – участников уголовно-процессуальных отношений. Тем самым запрещается применение мер, способных привести к приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей, на что

[1] При этом порядок такого осмотра и выемки не установлен, а он никак не может быть полностью аналогичен порядку, установленному ст. 185 УПК РФ.

[2] *Гаврилин Ю. В., Победкин А. В.* Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы // Труды Академии управления МВД России. 2018. № 3 (47). С. 110.

[3] *Гаврилин Ю. В., Победкин А. В.* Указ. соч. С. 110.

обращалось внимание в Послании Президента Российской Федерации Федеральному Собранию Российской Федерации от 01.03.2018.

Заметим, что правоприменители восприняли данную новеллу довольно настороженно. Проведенное нами исследование показало, что 77,3 % опрошенных сотрудников считают, что копирование не может быть приоритетным способом изъятия информации на электронных носителях, лишь 22,6 % опрошенных согласились с целесообразностью копирования как приоритетного способа изъятия информации на электронных носителях (не только при производстве по уголовным делам в сфере экономической и предпринимательской деятельности), пояснив, что оригинал необходим владельцу носителя, а также что копирование исключит изъятие большого количества носителей[1].

2. Определен исчерпывающий перечень исключений, позволяющих осуществлять изъятие электронных носителей информации по уголовным делам преступлениях в сфере экономической и предпринимательной деятельности, который будет рассмотрен ниже.

3. Установлено, что каждое изъятие электронных носителей информации должно осуществляться с участием специалиста.

Анализ практики применения новых положений уголовно-процессуального законодательства в части собирания доказательств на электронных носителях информации свидетельствует о наличии комплекса проблем правоприменения, связанных с их реализацией. В число данных проблем входят:

а) установление оснований для изъятия электронных носителей информации при производстве следственных действий, особенно по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности;

б) императивное требование участия специалиста;

в) обеспечение реализации права на копирование информации, содержащейся на изъятых электронных носителях.

Рассмотрим практику разрешения обозначенных проблем более подробно.

Говоря о правовых основаниях для изъятия электронных носителей информации, нами выше уже отмечалось, что по общему правилу по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности оно не допускается, за исключением следующих случаев.

[1] Нельзя не отметить, что настороженность правоприменителя в значительной степени может быть обусловлена и явно неудовлетворительной юридической техникой, использованной при формулировании ч. 4.1 ст. 164 УПК, и очевидной неясностью ряда положений ч. 1 ст. 164.1 УПК.

Первое исключение. *Изъятие допустимо в случае, если вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации.* Представляется, что указанное основание является трудно реализуемым на практике. В соответствии с п. 4 ч. 1 ст. 195 УПК РФ в постановлении о назначении экспертизы указываются материалы, предоставленные в распоряжение эксперта. Соответственно, на момент вынесения данного постановления в распоряжении следователя уже должны быть указанные материалы (в данном случае – электронные носители информации). Очевидно, что обеспечить наличие еще не изъятых материалов не представляется возможным. Кроме того, согласно ч. 3 ст. 195, ч. 1 ст. 198 УПК РФ и правовой позиции Верховного Суда, заинтересованные лица должны быть ознакомлены с постановлением о назначении экспертизы до ее производства[1].

В этой связи формальным основанием для вынесения постановления о назначении судебной экспертизы является протокол следственного осмотра, обыска, выемки, в ходе которых были обнаружены, зафиксированы и изъяты объекты для намечающегося исследования – электронные носители информации[2]. Соответственно, выполнение указанных требований процессуального закона в отношении не изъятых электронных носителей также не представляется возможным.

Второе исключение. *Изъятие электронных носителей информации производится на основании судебного решения.*

Полномочия суда закреплены в ст. 29 УПК РФ, ч. 2 которой предусматривает перечень решений, принимаемых судом в ходе досудебного производства. При этом решения суда об изъятии электронных носителей информации в данном перечне не содержится. Можно предположить, что применительно к п. 2 ч. 1 ст. 164.1 УПК РФ основаниями для изъятия электронных носителей информации выступают решения суда, указанные в п. 5 ст. 29 УПК РФ – о производстве обыска и (или) выемки в жилище, в ходе которых происходит изъятие электронных носителей информации, а также в п. 7 ст. 29 УПК РФ – о производстве выемки предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, а также предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кре-

[1] О судебной экспертизе по уголовным делам: постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28. П. 9 // Доступ из справ.-правовой системы «КонсультантПлюс».

[2] *Васюков В.Ф.* Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. № 2. С. 9.

дитных организациях, которые могут содержаться на электронных носителях информации, в связи с чем подлежат изъятию.

Данный вывод подкрепляется сложившейся судебной практикой рассмотрения жалоб на действия следователя при изъятии и осмотре информации с мобильных телефонов, в которых может храниться информация, относящаяся к охраняемой законом тайне.

Так, в Кассационном определении Омского областного суда указывалось, что ст. 13 УПК РФ предусмотрено, что ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений (к которым можно отнести и SMS-сообщения) допускается только на основании судебного решения. Более того, тайна личной переписки гарантирована и ч. 2 ст. 23 Конституции Российской Федерации, согласно которой каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. Кроме того, в ст. 8 Конвенции о защите прав человека и основных свобод указано, что каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции. Несмотря на то, что гл. 25 УПК РФ прямо не закрепляет обязанность следователя получать судебное разрешение на осмотр SMS-переписки, эта обязанность вытекает как из других норм уголовно-процессуального закона и положений Конституции Российской Федерации, так и из международных правовых норм, закрепленных в вышепоименованной Конвенции, подлежащих безусловному применению в Российской Федерации[1].

Судом было принято решение об отмене действий следователя по производству выемки и осмотру предметов и решения заместителя прокурора.

Приведенная позиция в определенной степени нашла свое отражение и в определении Конституционного Суда Российской Федерации от 28.02.2017 № 338-О, в котором отмечается, что если в ходе осмотра мобильного телефона владелец самостоятельно сообщает, что на нем установлен пароль, и кроме того, согласен представить распечатку телефонных соединений с используемого им номера, не возражает против проведения исследования имеющейся в телефоне информации, то нарушение конституционного права не усматривается[2]. Соответственно, в противном случае, когда собственник воз-

[1] Кассационное определение № 22-2225/12 Омского областного суда от 24.05.2012 по делу № 22-2225/12.

[2] Об отказе в принятии к рассмотрению жалобы гражданина Попова Анатолия Николаевича на нарушение его конституционных прав статьями 176 и 177 Уголовно-процессуального кодекса Российской Федерации: определение Конституционного Суда

ражает против проведения исследования своего гаджета без наличия судебного решения, возможно нарушение его конституционных прав.

В данном контексте заслуживает особого внимания позиция Конституционного Суда Российской Федерации, выразившаяся в определении от 25.01.2018 № 189-О, в котором указано, что проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения. Если же лица полагают, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения могут причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, они могут оспорить данные процессуальные решения и следственные действия в суде в порядке, предусмотренном ст. 125 УПК РФ[1].

Схематичность позиции Конституционного Суда Российской Федерации приводит к тому, что вопрос о необходимости вынесения отдельного судебного решения на изъятие электронных носителей информации вне процедур, предусмотренных ст. 29 УПК РФ, в частности при проведении осмотра информационного содержимого мобильных устройств систем связи (мобильных телефонов, коммуникаторов, смартфонов), в следственной и судебной практике разрешается неоднозначно.

Так, например, следователь обратился в суд с ходатайством о разрешении осмотра сведений, находящихся на электронных носителях информации, принадлежащих В. Постановлением Фрунзенского районного суда г. Владивостока от 15 апреля 2016 г. ходатайство следователя оставлено без удовлетворения. В апелляционном представлении прокурор Приморского края просил постановление суда отменить, ходатайство следователя о разрешении осмотра сведений, находящихся на электронных носителях информации, а также мобильных телефонах обвиняемого В., удовлетворить. Цитируя положения ст. 13, 29 и 165 УПК РФ, а также ст. 23 Конституции Российской Федерации, прокурор сослался на то, что ограничение права гражда-

---

РФ от 28 февраля 2017 г. № 338-О // Доступ из справ.-правовой системы «КонсультантПлюс».

[1] Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации: определение Конституционного Суда РФ от 25 января 2018 г. № 189-О // Доступ из справ.-правовой системы «КонсультантПлюс».

нина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений (к которым можно отнести и SMS-сообщения) допускается только на основании судебного решения. С учетом отсутствия согласия В. на осмотр электронных носителей предположил, что следователь обоснованно обратился в суд с ходатайством о разрешении производства осмотра предметов, изъятых у В. При этом настаивал на том, что отказ суда в удовлетворении ходатайства следователя может повлечь нарушение прав В. на тайну переписки, предусмотренных ч. 2 ст. 23 Конституции Российской Федерации, а также привести к получению следственным органом недопустимого доказательства, имеющего решающее значение для установления обстоятельств, предусмотренных ст. 73 УПК РФ.

Проверив представленные материалы, изучив доводы апелляционного представления, выслушав участвующих лиц, апелляционный суд не нашел оснований усомниться в правильности решения суда первой инстанции в связи с тем, что осмотр сведений, находящихся на электронных носителях информации, изъятых у В., производится следователем в соответствии со ст. 176 УПК РФ и для этого не требуется судебного решения[1].

Однако в правоприменительной практике встречаются и противоположные решения[2].

Таким образом, полагаем, что электронные носители информации могут быть изъяты в соответствии с п. 2 ч. 1 ст. 164.1 УПК РФ только при проведении следственных действий, перечень которых приведен в ст. 29 УПК РФ. При этом законодателю целесообразно уточнить свою позицию относительно смысла п. 2 ч. 1 ст. 164.1 УПК РФ.

Третье исключение. *На электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает.*

Примечательно, что в данном случае законодатель позволяет изымать электронные носители у лиц, которые могли быть непричастными к совершению расследуемых противоправных действий, но обладающих информацией, содержащейся на электронных носителях, без достаточных к тому правовых оснований. Такой информацией может являться, например, операционная система Windows, на которую у пользователя нет лицензии, или срок действия которой истек, либо иной другой программный продукт, не относящийся к

[1] Апелляционное постановление Приморского краевого суда от 31 мая 2016 г. по делу № 22-3453/2016.

[2] Постановление Сковородинского районного суда Амурской области от 19 декабря 2017 г. по делу № 3/12-65/2017.

свободно распространяемому программному обеспечению. Сказанное, на наш взгляд, открывает неоправданно широкие возможности для изъятия электронных носителей информации в обозначенных выше случаях. При этом не в полной мере достигаются цели, ради которых законодателем принимались анализируемые поправки.

Вероятно, законодатель имел в виду ситуации, при которых владелец не имеет право на хранение и использование информации, исходя из ее содержания. Например, это содержание представляет собой какую-либо охраняемую законом тайну. В случае, если хранить информацию и пользоваться ею, исходя из ее содержания, не запрещено, то рассматриваемое исключение не позволяет изымать электронные носители информации при производстве по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности даже в том случае, когда ее изъятие не влияет на осуществление указанной деятельности. Очевидно, что и в данном случае законодателю необходимо уточнять свою позицию с учетом того, что ч. 1 ст. 164.1 УПК РФ направлена на обеспечение нормального осуществления именно экономической и предпринимательской деятельности.

Четвертое исключение. *Информация, содержащаяся на электронных носителях, может быть использована для совершения новых преступлений.* Свидетельством такого использования может стать информация, полученная в результате проведения оперативно-розыскных мероприятий, первоначальных следственных действий, а также сведения о способе реализации преступного замысла фигурантами.

Так, например, при проведении обыска по уголовному делу, возбужденному по ч. 2 ст. 273 УК РФ, ч. 4 ст. 159.6 УК РФ, в квартире у одного из участников организованной группы было обнаружено 23 мобильных телефона, 17 USB-модемов, 370 SIM-карт, 6 ноутбуков, которые использовались для реализации преступной схемы по хищению денежных средств с дебетовых и кредитных банковских карт, а также с лицевых счетов абонентских номеров. В ходе расследования было установлено, что подозреваемые при непосредственном манипулировании с SIM-картами, используя специализированное программное обеспечение, осуществляли массовую рассылку SMS-сообщений на абонентские номера неустановленного круга лиц, содержащих ссылку на интернет-ресурс (сайт), на котором данной организованной преступной группой заранее была размещена вредоносная компьютерная программа, детектируемая антивирусным программным обеспечением.

После успешной установки в качестве приложения в операционной системе на базе Android в зараженном телефоне указанная программа

осуществляла контроль отправки, приема, а также отображения SMS-сообщений, как правило, направляемых с сервисных номеров банков, платежных систем, сотовых операторов и т. п. Затем используемая участниками организованной группы программа производила периодическое подключение к управляющему серверу с целью получения команд для выполнения, а также отправки собранной информации.

При этом участники организованной преступной группы осуществляли отслеживание в административной панели мобильных телефонов, на которые успешно установлено вредоносное программное обеспечение в формате «apk», после чего осуществляли хищения денежных средств путем отправления коротких команд на сервисные номера организаций.

Далее, после осуществления хищения денежных средств с расчетных счетов банковских карт и лицевых счетов абонентских номеров, данные денежные средства фигурантами переводились на расчетные счета банковских карт, оформленных на третьих лиц, находящиеся в распоряжении участников организованной преступной группы, а также на Киви-кошельки, Альфа-кошельки и Яндекс-кошельки, подконтрольные участникам группы. С целью конспирации участники группы производили хищения в арендованных квартирах, расположенных в различных регионах России[1].

Пятое исключение. *Копирование информации по заявлению специалиста может повлечь за собой ее утрату или изменение.* При осуществлении изъятия электронных носителей вывод о возможной утрате или изменении информации делается только специалистом, участвующим в следственном действии. При этом данный вывод выражается в заявлении, которое фиксируется в протоколе следственного действия, в ходе которого осуществлялось изъятие. Отсутствие соответствующей записи о том, что копирование не может быть осуществлено в связи с возможной утратой или изменением информации, является основанием признания недопустимыми действий лиц, осуществляющих изъятие электронных носителей информации.

Рассмотрим позицию Верховного Суда Республики Адыгея, который обращает внимание на то, что следователь перед изъятием в присутствии специалиста обязан проверить, «что 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 кото-

[1] Приговор Московского районного суда г. Чебоксары Чувашской Республики от 3.08.2018 г. по делу 1-180/2018.

рой, по заявлению специалиста, может повлечь за собой ее утрату или изменение». С учетом изложенного, постановление Майкопского городского суда о признании законным производство обыска в жилище, занимаемом Б., отменено, дело направлено на новое рассмотрение в тот же суд в ином составе[1].

Существенные проблемы правоприменения влекут формулировки ч. 2 ст. 164.1 УПК РФ об обязательном участии специалиста при изъятии электронных носителей информации. Такие формулировки ранее уже использовались в утративших силу нормах ч. 91 ст. 182 и ч. 31 ст. 183 УПК РФ. При этом требование обязательного привлечения для изъятия электронных носителей информации специалиста тесно связано с обозначенной выше проблемой отсутствия в уголовно-процессуальном законе определения понятия электронного носителя информации. При буквальном толковании требование об обязательном участии специалиста подлежит применению при изъятии любых других устройств, обладающих внутренней памятью, содержащей информацию в электронно-цифровой форме, даже в случае, когда находящиеся на них сведения не имеют значения для расследования. Кроме того, обязательность участия специалиста не обусловлена следственной практикой, т. к. в большинстве случаев следователи обладают необходимыми познаниями для изъятия электронных носителей информации, на что обращают внимание сами сотрудники органов расследования преступлений[2].

При этом имеет место неоднозначная практика применения указанных норм.

Так, например, в одном случае судами делается вывод о том, что участие специалиста обязательно только при копировании информации, содержащейся на изъятых предметах[3].

В другом случае Судебной коллегией по уголовным делам Рязанского областного суда дается пояснение, что «участие специалиста в производстве выемки в ходе изъятия электронных носителей информации требуется при наличии нуждаемости в данном специалисте. Фактически, при проведении выемки не осуществлялось изъятие электронных носителей, а осуществлялось копирование имею-

---

[1] Апелляционное постановление Верховного Суда Республики Адыгея от 13.06.2019 по делу № 22-316.

[2] Письмо СУ УМВД России по Рязанской области от 16.07.2019 № 16/6863.

[3] Апелляционное постановление Приморского краевого суда от 24.10.2017 по делу № 22-5439/2017; Апелляционное постановление Тульского областного суда от 12.02.2018 по № 22-122; Апелляционное постановление Самарского областного суда от 10.12.2018 по делу № 22-7165/2018; Апелляционное определение Брянского областного суда от 11.04.2019 по делу № 22-400/2019; Апелляционное определение суда Чукотского автономного округа от 28.05. 2019 по делу № 1-5/2019 (22-38/2019); Апелляционное определение Томского областного суда от 11.06.2019 по делу № 22-1217/2019.

щейся информации на отдельный носитель, что не запрещено нормами УПК РФ и не требует обязательного привлечения специалиста»[1].

В третьем случае Судебная коллегия по уголовным делам Ярославского областного суда признает отсутствие специалиста допустимым при проведении следственных действий, так как «электронные носители информации изымались целиком, то есть без проверки и изъятия самой информации», что не дает суду оснований усомниться в достоверности информации, которая впоследствии может быть обнаружена в этом носителе[2].

В четвертом случае Судебная коллегия по уголовным делам Верховного Суда Республики Хакасия посчитала необоснованными и не подлежащими удовлетворению доводы апелляционной жалобы о нарушении при обыске положений об обязательном участии специалиста, поскольку, по мнению судей, «применение специальных познаний и навыков при изъятии компьютерного блока, составной частью которого является электронный носитель информации, без его вскрытия или копирования не требовалось»[3].

В пятом случае Ленинградский областной суд указывает на то, что «из материалов уголовного дела следует, что фактически необходимость в привлечении к участию специалиста отсутствовала, поскольку и мобильные телефоны, и персональные компьютеры изымались лишь как предметы, копирование информации с изымаемых устройств не производилось и, как правильно указал суд, риск повреждения и уничтожения содержащейся на них информации отсутствовал»[4].

В шестом случае на заявление подсудимого о том, что недопустимыми доказательствами является видеозапись на CD-диске из-за копирования информации с электронного носителя без участия специалиста, Новосибирский областной суд поясняет следующее: «... данных, свидетельствующих о наличии признаков монтажа видеозаписи, по делу не установлено. То обстоятельство, что видеозапись была перенесена с помощью записи на камеру телефона и на внешний носитель компакт-диска без участия специалиста, на что указывается в жалобе, не свидетельствует о порочности вышеуказанного доказательства, поскольку электронный носитель информации не изымал-

[1] Апелляционное определение Рязанского областного суда от 03.04.2018 по делу № 22-148/2018.

[2] Апелляционное определение Судебной коллегии по уголовным делам Ярославского областного суда от 11.07.2017 по делу № 22-968/2017.

[3] Апелляционное определение Верховного Суда Республики Хакасия от 13.12.2018 по делу № 22-1516/2018.

[4] Апелляционное определение Ленинградского областного суда от 04.07.2019 по делу № 22-1092/2019.

ся, применение специальных познаний и навыков при копировании записи на телефон и компакт-диск не требовалось, в связи с чем оснований для привлечения специалиста не имелось»[1].

Отдельно хотелось бы отметить позицию Вологодского областного суда, который в своем апелляционном решении соглашается с судом первой инстанции и резюмирует, что «мобильный телефон является средством мобильной связи, не предназначен исключительно для накапливания и хранения информации». При этом, по мнению суда, если при обнаружении сотового телефона копирование информации на другие электронные носители не осуществляется, риска утраты или изменения данных не имеется, следовательно, применения специальных познаний и навыков не требуется[2].

Вместе с тем, при подобных обстоятельствах, решением Свердловского суда г. Белгорода года отменено постановление следователя о частичном отказе в удовлетворении ходатайства свидетеля и его адвоката. Последние заявили ходатайство о предоставлении возможности получения копий файлов с изъятых мобильных аппаратов связи. Доводы следователя о том, что «телефоны являются средствами мобильной связи, не предназначенными исключительно для накапливания, хранения и воспроизведения данных, в связи с чем их нельзя признать электронными носителями», суд посчитал несостоятельными. Таким образом, суд фактически признал мобильные телефоны электронными носителями информации. Суд апелляционной инстанции оставил данное решение без изменения[3].

Приведенные примеры наглядно демонстрируют отсутствие единства правоприменительной практики по вопросу участия специалиста при изъятии электронных носителей информации.

Анализируя обозначенную проблему, отметим, что в отличие от ранее действующих норм ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ, предусматривающих изъятие с обязательным участием специалиста только при обыске и выемке, положения ч. 2 ст. 164.1 УПК РФ касаются всего спектра следственных действий. Иными словами, исходя из содержания ч. 2 ст. 164.1 УПК РФ при производстве любого следственного действия, производимого следователем или органом дознания, участие специалиста обязательно в случае изъятия флэш-носителей, ноутбуков (нетбуков, ультрабуков), видеорегистраторов, системных бло-

---

[1] Апелляционное определение Новосибирского областного суда от 08.07.2019 по делу № 22-3319/2019.

[2] Апелляционное определение Вологодского областного суда от 24.07.2018 по делу № 22-1245/2018.

[3] Письмо СУ УМВД России по Белгородской области от 15.08.2019 № 18/940.

ков, сотовых телефонов, смартфонов всех видов и типов, планшетных устройств, компьютерных блоков (моноблоков) и других менее распространенных электронных носителей информации. Сказанное касается как проведения следственных действий с участием как подозреваемых (обвиняемых), так и свидетелей (потерпевших).

Обращаем внимание, что игнорирование нормы об участии специалиста при изъятии электронных носителей информации может повлечь самые негативные последствия для доказывания. Так, апелляционным постановлением Московского областного суда от 22.01.2019 была удовлетворена жалоба С., поданная в порядке ст. 125 УПК РФ, на незаконные действия следователя СУ УМВД России по городскому округу Королев о незаконном изъятии в ходе обыска в нежилом помещении документов и компьютеров, содержащих базы данных 1С, принадлежащих ООО «...». Мотивируя свое решение, суд указал, что процессуальная самостоятельность следователя, регламентированная ст. 38 УПК РФ, не подлежит сомнению, однако, принимая во внимание, что действия следователя должны носить законный характер, а лицо, считающее свои права и интересы нарушенными, может обжаловать такие действия в порядке ст. 125 УПК РФ, суду первой инстанции следовало надлежащим образом проверить доводы заявителя, учтя при этом, что ст. 81.1, 164, 164.1 УПК РФ предусматривают особый порядок изъятия предметов и документов, включая электронные носители информации, признания их вещественными доказательствами по уголовным делам о преступлениях, предусмотренных ст. 196 УК РФ[1].

Таким образом, в силу того, что единое применение данного положения ч. 2 ст. 164.1 УПК РФ региональными судебными органами до настоящего времени не сформировано, при необходимости изъятия электронных носителей информации бытового использования (оптических дисков, флэш-накопителей, ноутбуков, мобильных телефонов (смартфонов), видеорегистраторов и др.) привлечение специалиста обеспечивается в зависимости от сложившейся региональной судебной практики, а также позиции органов прокуратуры.

Организационными проблемами, возникающими при реализации требований ст. 81.1, 164.1 УПК РФ, по результатам проведенного авторами опроса практических сотрудников и руководителей органов расследования преступлений, являются недостаточное количество специалистов, образование, опыт работы и квалификация которых позволяет им участвовать в следственных действиях, сопряженных с изъятием электронных носителей информации,

[1] Апелляционное постановление Московского областного суда от 22.01.2019 по делу № 22к-476/2019.

и необеспеченность следственных подразделений съемными жесткими дисками большой емкости для обеспечения возможности копирования информации без изъятия электронных носителей[1].

При этом следует обратить внимание, что вопрос о степени компетентности лица, привлекаемого в качестве специалиста для изъятия электронных носителей информации, относится на усмотрение должностного лица, проводящего следственное действие. Так, Апелляционным судом г. Севастополя была оставлена без удовлетворения жалоба о нарушении требований УПК РФ в части привлечения специалиста при изъятии электронного носителя информации. Из содержания обжалуемого протокола следует, что при обыске в качестве специалиста присутствовал оперуполномоченный, который заявил, что на электронных носителях информации, находящихся в месте производства обыска, содержится информация, копирование которой может повлечь за собой ее утрату или изменение. При таком положении, в соответствии с п. 3 ч. 1 ст. 164 УПК РФ, следователем произведено изъятие электронного носителя информации. Суд признал несостоятельными доводы апелляционной жалобы о том, что оперуполномоченный, принимавший участие в качестве специалиста, не имеет специального образования, стажа и навыков работы в сфере информационных и компьютерных технологий, а также о том, что он заинтересованное лицо, так как является оперативным сотрудником УМВД России по г. Севастополю. При этом судом принято во внимание, что в материалах имеется приложение к диплому об образовании, свидетельствующее о том, что данный сотрудник обладает специальными познаниями в области компьютерных технологий[2].

Следует также отметить, что в научной литературе требование уголовно-процессуального законодательства об обязательном участии специалиста при изъятии электронных носителей информации подвергается справедливой критике. Так, по мнению К. А. Костенко, участие специалиста в изъятии обнаруженных на месте обыска или в ходе выемки различных накопителей на жестких магнитных дисках, карт флэш-памяти, компакт-дисков, сотовых телефонов, цифровых фотоаппаратов, mp3-плееров является излишним[3]. По мнению вышеназванного автора, такие объекты без ущерба для проведения

---

[1] Письмо СУ УМВД России по Брянской области от 22.07.2019 № 17/8587.

[2] Апелляционное постановление Севастопольского городского суда от 06.05.2019 по делу № 22К-277/2019.

[3] *Костенко К. А.* К вопросу об особенностях изъятия электронных носителей информации при расследовании служебных преступлений // Служебные преступления: вопросы теории и практики правоприменения: сб. материалов Междунар. науч.-практ. конф. (17 мая 2018 г., г. Хабаровск) / под ред. Т. Б. Басовой, К. А. Волкова. Хабаровск: Юрист, 2018. С. 7.

расследования и интересов владельцев могут быть самостоятельно изъяты и упакованы следователем.

Авторами настоящего пособия также ранее отмечалось, что законодательное требование об обязательном участии специалиста при проведении обыска или выемки, в ходе которых осуществляется изъятие электронного носителя информации, выглядит «чрезмерным и неоправданным»[1]. Приведенную позицию разделяют и многие другие авторы[2].

Действительно, далеко не всегда производство следственных действий, в ходе которых изымаются электронные носители информации, сопряжено с исследованием содержащейся на них информации. Данная задача может решаться в рамках отдельного следственного действия – осмотра предметов, для проведения которого может (и должен!) быть приглашен специалист в области информационно-телекоммуникационных технологий. Соответственно, основной задачей специалиста при производстве следственных действий, в ходе которых изымаются электронные носители информации, является обеспечение достоверности полученных доказательств – неизменности информации, содержащейся на изымаемом носителе, что достигается соблюдением процессуальных требований и криминалистических рекомендаций к порядку его упаковки и изъятия[3]. На практике участие специалиста при изъятии электронных носителей выражается в их упаковывании в ходе следственного действия, а также правильном описании носителя в протоколе. Большинство опрошенных работников правоохранительных органов (75,3 %) также отметили, что счита-

---

[1] *Гаврилин Ю.В.* Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4. С. 47; *Гаврилин Ю. В., Победкин А.В.* Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы // Труды Академии управления МВД России. 2018. № 3 (47). С. 109.

[2] *Зуев С.В.* Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С. 58; *Клевцов В.В.* Проблемные аспекты изъятия электронных носителей информации при расследовании распространения «дизайнерских» наркотиков с использованием сети Интернет // Российский следователь. 2015. № 6. С. 12; *Старичков М.В.* Вопросы использования носителей компьютерной информации в качестве доказательств // Известия Тульского государственного университета. 2017. № 2. С. 119.

[3] Более подробно см.: *Жердев П.А.* Тактические особенности изъятия электронных носителей информации // Вестник Дальневосточного института МВД России. 2015. № 4. С. 98; *Мещеряков В. А.* Цифровая криминалистика // Библиотека криминалиста. 2014. № 4. С. 231–241; *Осипенко А. Л., Гайдин А.И.* Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. № 1. С. 157.

ют неоправданной норму об участии специалиста в каждом случае изъятия электронных носителей информации в ходе обыска или выемки.

В этой связи полагаем, что требование УПК РФ об обязательности участия специалиста в ряде случаев вызывает сомнение, в частности, когда речь идет об изъятии съемных энергонезависимых электронных носителей, которое не представляет сложностей ни с технической, ни с процессуальной точки зрения. Полагаем, что на современном уровне распространения цифровых технологий в повседневной жизнедеятельности обладание навыками использования применяемых в бытовых целях электронных носителей не является специальными знаниями, а относится к общераспространенным, обыденным знаниям.

С учетом изложенного, считаем необходимым внесение изменений в УПК РФ в указанной части, предоставив следователю самостоятельно решать вопрос о необходимости привлечения специалиста к изъятию электронных носителей информации в зависимости от реальной необходимости в использовании специальных знаний.

Заметим, что подобный подход встречается и в судебной практике. Так, Красноярский краевой суд, рассмотрев апелляционную жалобу на постановление судьи Минусинского городского суда Красноярского края, установил, что в рамках расследования уголовного дела было произведено изъятие электронных носителей информации, в процессе которого, в соответствии со ст. 164.1 УПК РФ, необходимо присутствие специалиста. Однако, как следует из представленных материалов, в ходе обыска в жилище электронные носители информации изымались целиком, без проведения их осмотра на предмет содержащейся на них информации, а также без проверки и изъятия самой информации. Изъятые электронные носители в присутствии понятых были упакованы и опечатаны для достоверности информации, которая впоследствии может быть обнаружена в этих носителях. В связи с изложенным доводы апелляционной жалобы заявителя о недопустимости отсутствия специалиста при изъятии электронных носителей информации суд апелляционной инстанции считает необоснованными[1].

Еще одной процессуальной проблемой существующего порядка регламентации следственных действий, в ходе которых происходит изъятие электронных носителей информации, является реализация закрепленного в ч. 2 ст. 164.1 УПК РФ права законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации на выполнение копирования информации с изымаемых электронных носителей, которое производится

[1] Апелляционное постановление Красноярского краевого суда от 06.06.2019 по делу № 22К-3405/2019.

специалистом, участвующим в следственном действии, в присутствии понятых. Существующая правовая регламентация порядка реализации вышеназванного права содержит указание на то, что если в ходе следственного действия было получено ходатайство о копировании, то законный владелец изымаемых электронных носителей информации или обладатель содержащейся на них информации самостоятельно предоставляет специалисту электронные носители, на которые должно производиться копирование. По окончании данной процедуры электронные носители со скопированной на них информацией передаются законному владельцу изымаемых электронных носителей, о чем в протоколе делается соответствующая запись.

Необоснованный отказ в реализации законного требования владельца информации, содержащейся на изымаемом электронной носителе, является существенным нарушением уголовно-процессуального закона. Так, Камчатским краевым судом были признаны незаконными действия оперуполномоченного ОЭБ и ПК ОМВД РФ по Елизовскому району, выразившиеся в отказе в удовлетворении ходатайства генерального директора ОАО «...» С. о копировании информации, изымаемой с электронных носителей в ходе обыска.

Как следовало из представленных суду материалов, в протоколе обыска зафиксировано пояснение С. о том, что изъятие электронных носителей информации (жестких дисков) полностью парализует работу предприятия. В ходе судебного заседания С. подтвердил, что просил сотрудников полиции произвести копирование информации, изымаемой на электронных носителях, предлагал для этого свой свободный от информации электронный носитель, но ему было отказано. Он желал написать замечания об этом в протокол, но ему не позволили это сделать.

При этом суд апелляционной инстанции отметил, что данные пояснения С. ничем не опровергнуты. Сведений о том, что С. в ходе обыска было предложено скопировать изымаемую с электронных носителей информацию, а он от этого отказался, в протоколе не имеется. Запись в протоколе обыска о том, что у С. отсутствуют замечания к протоколу, не означает, что заявитель не ходатайствовал о копировании изымаемой информации.

Учитывая, что в протоколе обыска не имеется сведений, указывающих на то, что копирование информации, изъятой с электронных носителей, может воспрепятствовать расследованию или повлечь ее утрату или изменение, суд апелляционной инстанции пришел к выводу о том, что действия должностного лица, проводив-

шего обыск, не отвечают в полной мере положениям, закрепленным уголовно-процессуальным законодательством[1].

Заметим, что копирование в данном случае – это часть следственного действия, а не самостоятельное процессуальное действие. Вместе с тем, в настоящее время в литературе обсуждается вопрос о признании копирования информации с электронного носителя самостоятельным следственным действием.

Так, В. А. Семенцов полагает, что в практике расследования уголовных дел все чаще возникает необходимость копирования доказательственной информации, и этот новый познавательный прием соответствует требованиям закона, морали и социальным закономерностям общественного развития. При этом необходимо включить электронное копирование в систему процессуальных действий, предназначенных для собирания доказательств[2].

На выделении копирования в качестве отдельного следственного действия также настаивают С. В. Зуев и Д. В. Овсянников, отмечая при этом, что любое средство доказывания может быть как отдельным следственным действием, так и частью следственного действия[3].

Полагаем, что данный подход не может быть поддержан в связи с тем, что при изготовлении копии информации с изымаемых носителей по ходатайству их законного владельца новое доказательство не формируется, что не позволяет отнести данную процедуру к числу следственных действий. Фактически речь идет о случаях изъятия электронных носителей информации в ходе самостоятельного следственного действия, а скопированная информация передается законному владельцу электронных носителей информации или обладателю содержащейся на них информации.

Однако возникает серьезная практическая проблема: каким образом обеспечить участие понятых в ситуации возникновения необходимости копирования информации с электронных носителей в ходе осмотра или выемки, при производстве которых, как известно, участие понятых не обязательно, а участие понятых должно быть обеспечено с начала производства следственного действия. Должностным лицам, осущест-

---

[1] Апелляционное постановление Камчатского краевого суда от 13.03.2018 по делу № 22к-160/2018.

[2] *Семенцов В. А.* Следственные действия в досудебном производстве (общие положения теории и практики): монография. Екатеринбург, 2006. С. 300.

[3] *Макаров М. А.* Копирование содержимого электронных носителей как средство доказывания в электронном процессе // Молодой ученый. 2019. № 1. С. 109–110. URL: https://moluch.ru/archive/239/55327/ (дата обращения: 04.02.2020); *Зуев С. В.* Электронная информация и ее носители в уголовно-процессуальном доказывании: развитие правового регулирования // Вестник ЮУрГУ. Серия: Право. 2017. № 1. Т. 17. С. 32.

вляющим предварительное расследование, можно рекомендовать обеспечивать участие понятых при производстве следственных действий, в ходе которых может возникнуть необходимость изъятия электронных носителей информации. Такая возможность предусмотрена ч. 11 ст. 170 УПК. При отсутствии понятых при производстве следственного действия необходимость копирования с электронных носителей информации влечет приостановление производства следственного действия, приглашение понятых, разъяснение им прав и обязанностей, возобновление следственного действия и проведение копирования информации.

По данным проведенного нами исследования, в ходе изучения уголовных дел было выявлено, что в 70 % дел ходатайство о копировании информации с изымаемых электронных носителей, от законного владельца информации или обладателя содержащейся на них информации, в ходе проведения следственных действий не поступало, в 25 % случаев ходатайство поступало, но в его удовлетворении было отказано.

Кроме того, в 84 % изученных уголовных дел копирование информации с изымаемых электронных носителей по ходатайству законного владельца информации или обладателя содержащейся на них информации специалистом, участвующим в обыске, выемки не осуществлялось, в 16 %, соответственно, – копирование было произведено.

Несмотря на то, что ч. 3 ст. 164.1 УПК предусматривает возможность копирования информации, содержащейся на электронных носителях, для приобщения к материалам уголовного дела именно скопированной информации, правоприменитель предпочитает изъятие. Полагаем, что «популярность» изъятия электронных носителей по отношению к копированию информации обусловлена следующим:

1) сокращение временных затрат на процедуру копирования, которая может занять большее количество времени;

2) возможность более тщательного осмотра и изучения изъятых носителей и информации на ней в рамках последующих следственных действий;

3) отсутствие рисков, связанных с возможностью уничтожения информации ее владельцем;

4) снижение рисков, связанных с возможностью выхода из строя носителей со скопированной информацией при их транспортировке.

Относительно участия специалиста при производстве копирования изымаемой информации отметим следующее. Обязательное участие специалиста требуется лишь при изъятии электронных носителей, а также копировании с них информации для передачи информации, скопированной на электронный носитель, законному владельцу электронных носителей или обладателю содержащейся на них информации (ч. 2 ст. 164.1 УПК). При производстве копирования для приобще-

ния к уголовному делу именно тех носителей информации, на которые информация была скопирована (ч. 3 ст. 164.1 УПК), участие специалиста не предусмотрено. Вместе с тем, полагаем, что именно в данном случае участие специалиста необходимо, что обусловлено обеспечением тождественности изымаемой и копируемой информации (равно как и в случае копирования, предусмотренном ч. 2 ст. 164.1 УПК).

Подобная ситуация может быть проиллюстрирована следующим примером. Приговором Калининского районного суда недопустимыми доказательствами была признана видеозапись на CD-диске в связи с копированием информации с электронного носителя без участия специалиста. Однако суд апелляционной инстанции указал, что то обстоятельство, что видеозапись была перенесена с помощью записи на камеру телефона и на внешний носитель – компакт-диск – без участия специалиста, само по себе не свидетельствует о порочности вышеуказанного доказательства, поскольку электронный носитель информации не изымался, применение специальных познаний и навыков при копировании записи на телефон и компакт-диск не требовалось, в связи с чем оснований для привлечения специалиста не имелось[1].

Представляется, что здесь налицо некоторая непоследовательность законодателя. Не вполне понятно, в связи с чем требования к обеспечению достоверности доказательственной информации, получаемой в процессе ее копирования для материалов уголовного дела, ниже требований к достоверности информации, предоставляемой законному владельцу изымаемых носителей. Несмотря на то, что, по мнению отдельных авторов, предоставление следователю права самостоятельно копировать информацию с электронных носителей полностью соотносится с уровнем развития современных информационных технологий[2], полагаем, что для обеспечения единства правоприменения следует унифицировать подходы законодателя к вопросу об участии специалиста при изъятии электронных носителей.

В заключение параграфа отметим следующее.

1. Требование ч. 2 ст. 164.1 УПК РФ об обязательном участии специалиста при изъятии электронного носителя информации является излишним. Предлагается предоставить следователю, дознавателю право самостоятельно решать вопрос о целесообразности привлечения специалиста при изъятии электронного носителя информации с учетом его типа и технических особенностей.

---

[1] Апелляционное постановление Новосибирского областного суда № 22-3319/2019 от 08.07.2019 по делу № 1-47/2019.

[2] *Зуев С. В., Черкасов В. С.* Новые правила изъятия электронных носителей и копирования информации (статья 164.1 УПК РФ): преимущества и недостатки новеллы // Сибирское юридическое обозрение. 2019. № 2. Т. 16. С. 196.

2. Копирование информации как приоритетный способ изъятия электронного носителя информации по делам о преступлениях в сфере экономической и предпринимательской деятельности целесообразно распространить на производство по всем составам преступлений, установив при этом следующие основания для возможности их изъятия:

– отсутствие возможности исследования информации в ходе следственного действия;

– информация на электронном носителе отвечает требованиям, предъявляемым ч. 1 ст. 81 УПК РФ;

– 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.

Вопросы для повторения

1. Укажите основания для изъятия электронных носителей информации по действующему уголовно-процессуальному законодательству.

2. В каких случаях, по общему правилу, изъятие электронных носителей не допускается?

3. В каких случаях для изъятия электронных носителей информации требуется судебное решение?

4. К какому виду процессуальных действий относится копирование информации?

5. В каких случаях допускается копирование информации, содержащейся на электронных носителях, в ходе следственных действий?

6. Приведите перечень задач специалиста при изъятии электронных носителей информации.

Практическое задание

Опишите процессуальный порядок копирования информации с электронных носителей:

а) для целей ее изъятия;

б) по ходатайству законного владельца изымаемой информации и (или) ее носителя.

Глава 2. Особенности собирания, проверки и оценки информации на электронных носителях

§ 1. Собирание доказательственной информации на локальных и сетевых носителях: процессуальная регламентация и тактика

В соответствии со ст. 85 УПК РФ процесс доказывания включает в себя собирание, проверку и оценку доказательств в целях установления обстоятельств, входящих в предмет доказывания.

Одно из наиболее емких определений доказывания как познавательной деятельности по уголовному делу принадлежит С.А. Шейферу, понимавшему под доказыванием получение доказательств и оперирование ими в целях воссоздания действительной картины изучаемого события[1]. Познавательную сущность данного процесса отмечал в своих трудах профессор М.С. Строгович, указывавший, что процесс доказывания и есть процесс познания фактов, обстоятельств дела[2].

Исходя из законодательной дефиниции процесса доказывания, приведенной в ст. 85 УПК РФ, его содержанием являются собирание, проверка и оценка доказательств.

Рассмотрим содержание указанной деятельности применительно к доказательствам на электронных носителях информации.

В науке уголовного процесса традиционно считается, что собирание доказательств представляет собой систему действий, направленных на восприятие объективно существующих следов происшедшего события и их процессуальную фиксацию[3].

Понятию собирания доказательств посвящена ст. 86 УПК РФ. При этом законодатель не приводит определение процесса собирания доказательств, отмечая лишь, что оно осуществляется дознавателем, следователем, прокурором и судом путем производства следственных и иных процессуальных действий. Кроме того, в приведенной норме содержится также указание на процессуальные формы собирания сведений для подозреваемого, обвиняемого, а также потерпевше-

[1] *Шейфер С. А.* Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования. Москва: НОРМА, 2009.

[2] *Строгович М. С.* Курс советского уголовного процесса. Москва, 1958. С. 296.

[3] *Шейфер С.А.* Сущность и способы собирания доказательств в советском уголовном процессе. Москва: ВЮЗИ, 1972; *Шейфер С.А.* Собирание доказательств в советском уголовном процессе. Саратов: Саратов. ун-т, 1986. С. 54.

го, гражданского истца, гражданского ответчика, их представителей и *собирания доказательств* (курсив авторов) для защитника.

На самом деле, собирание доказательств представляет собой процессуально урегулированный процесс поиска, выявления и фиксации сведений, имеющих значение для уголовного дела. С. А. Шейфер формулирует комплексное определение собирания доказательств, которое отражает как гносеологическую, так и процессуальную сущность этого процесса. Собирание доказательств, как пишет он, – система действий, обеспечивающих восприятие субъектом доказывания объективно существующих следов изучаемого события, сопровождающихся формированием в сознании познавательного образа, а также действий, обеспечивающих сохранение этого образа, путем процессуальной фиксации результатов восприятия[1].

Фактически уполномоченное должностное лицо формирует доказательства, придавая процессуальную форму сведениям. В этой связи, невзирая на прямое указание в ст. 86 УПК на право защитника собирать доказательства и способы такого собирания, защитник, конечно, собирает лишь сведения, а не доказательства. Равно не собирают (не формируют) доказательства иные невластные участники уголовного судопроизводства.

Сущность процесса собирания доказательств состоит в их поиске, обнаружении, фиксации и изъятии содержащейся в них информации способами, установленными уголовно-процессуальным законом[2]. Каждому виду доказательства соответствует определенный способ собирания, оформления и закрепления информации в соответствующей процессуальной форме.

Обнаружение доказательств означает их отыскание, выявление, установление тех или иных фактических данных, имеющих доказательственное значение[3], – это начальная и необходимая стадия собирания доказательств.

Фиксация доказательств является составляющей процесса собирания доказательств. Обоснование этого мнения было приведено А. И. Винбергом еще в 1950 г., который указывал на фиксацию доказательств как на элемент процесса собирания доказательств, выражающуюся в их закреплении и запечатлении[4].

---

[1] *Шейфер С. А.* Собирание доказательств в советском уголовном процессе. Саратов, 1986. С. 24.

[2] *Белкин Р. С.* Криминалистическая энциклопедия. 2-е изд., доп. Москва: Мега-трон XXI, 2000. С. 211.

[3] *Белкин Р. С.* Собирание, исследование и оценка доказательств. Сущность и методы. Москва: Наука, 1966. С. 29.

[4] *Винберг А. И.* Криминалистика. Вып. 1: Введение в криминалистику. Москва, 1950. С. 8.

1. Особенности обнаружения электронных носителей информации. При проведении осмотра (обыска), где предполагается обнаружить электронные носители информации, следует учитывать, что они могут быть малы, легко скрыты, а иногда замаскированы, чтобы выглядеть как неэлектронный объект.

Для наиболее эффективного поиска следует:

1. Провести опрос присутствующих при следственном действии в целях добровольной выдачи носимых электронных носителей информации, мобильных устройств.

2. Ограничить доступ к имеющимся электронным носителям информации.

2. Проверить мониторы, модемы, другие устройства на наличие слотов для карт памяти.

3. Тщательно изучить брелоки, сумки, барсетки, часы присутствующих в помещении, где проводится следственное действие.

4. В случае проведения следственного действия в жилом помещении необходимо исследовать смарт-технику, телевизоры и любые персональные электронные устройства.

5. Изучению подлежат рабочая поверхность рабочих столов для обнаружения имен пользователей, паролей и учетных записей электронной почты.

Наиболее типичными упущениями при подготовке следственных действий, в ходе которых изымаются электронные носители информации, являются:

– отсутствие достоверной информации о точном местонахождении электронного оборудования, с которого может поступить команда для сокрытия или уничтожения интересующих следствие сведений;

– отсутствие достоверных сведений об организации локальной сети и размещении всех ее составляющих;

– отсутствие данных о степенях защиты информации, применяемых в организации или физическим лицом[1].

Эффективным тактическим приемом, используемым при проведении следственных действий, направленных на обнаружение электронных носителей информации, является применение средств радиоподавления, препятствующих возможности дистанционной подачи команд на уничижение (блокирование, модификацию) доказательственной информации с использованием беспроводных компьютерных сетей и сетей мобильной связи. Для целей обнаружения скрытых или замаскированных электронных носителей информации,

[1] Письмо ГСУ ГУ МВД России по г. Санкт-Петербургу и Ленинградской области от 06.08.2019 № 8/22989.

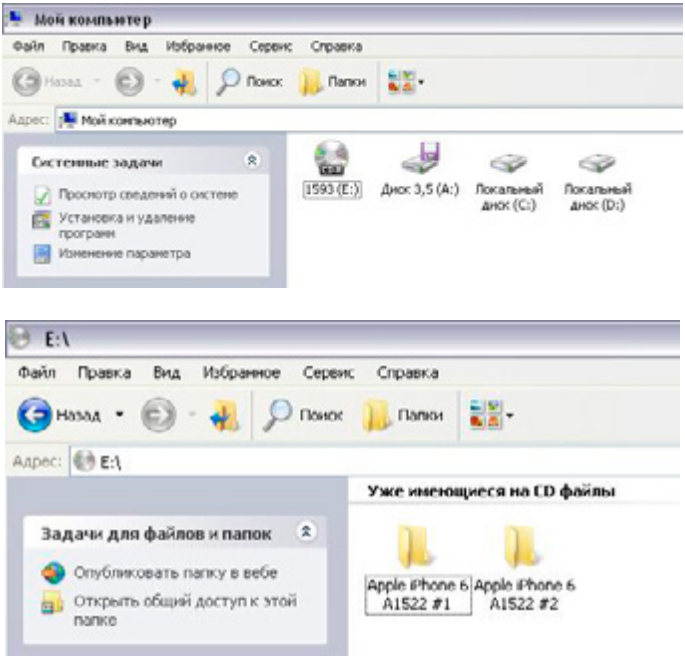
содержащих электронные компоненты, применяются нелинейные локаторы.

2. Тактика фиксации и изъятия электронных носителей информации. Изучение материалов уголовных дел показало, что следователями используются два способа фиксации осмотра электронного носителя информации.

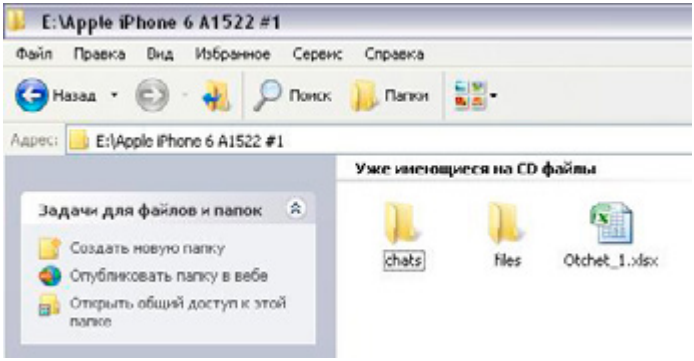
Первый способ предполагает отражать в описательной части протокола осмотра сделанные с помощью функции Print Screen изображения в хронологическом порядке.

Например: «...бумажный конверт белого цвета, на лицевой стороне которого имеется полиграфический текст, выполненный красителем черного цвета, следующего содержания: «ВЕЩЕСТВЕННОЕ ДОКАЗАТЕЛЬСТВО диск, являющийся приложением к заключению эксперта № 1593 от 29.05.2018, ст. следователь, подпись ...» Клапан осматриваемого конверта заклеен и опечатан отрезком бумаги белого цвета с оттиском печати «...СУ УМВД России по Тверской области...», заверенный тремя подписями.

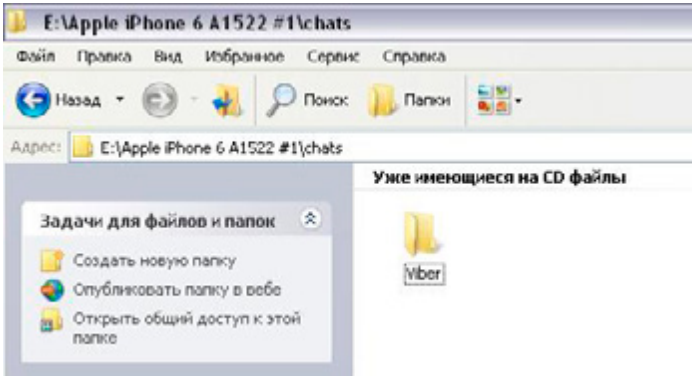
При вскрытии конверта в нем обнаружен диск «Verbatim CD-R», при воспроизведении которого обнаружено следующее:



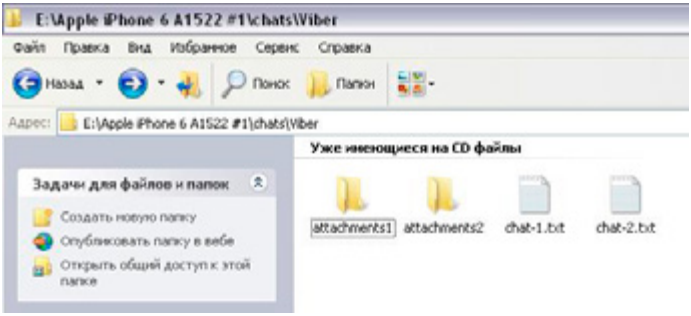
При воспроизведении системной папки с названием «Apple IPhone 6 A 1522 #1» обнаружена следующая информация:



При воспроизведении системной папки с названием «chats» обнаружена системная папка с названием «Viber»,



в которой обнаружены следующие системные папки и электронные документы:



В системной папке с названием «attachments1» обнаружена следующая, представляющая доказательственное значение, информация... [1]

Далее следователь добавляет в протокол изображения, находящиеся в обнаруженных папках *(рис. 1)*.

Рис. 1. Изображение, находящееся в обнаруженных папках

Второй способ предполагает фиксировать процесс осмотра электронного носителя информации в описательной части протокола только текстовую информацию. При этом все изготовленные изображения систематизируются в иллюстрационной таблице как приложения к протоколу.

Например: «...непосредственным объектом осмотра является бумажный конверт. На конверте имеются пояснительные надписи и подписи от имени понятых. Признаков нарушения целостности упаковка не имеет.

При вскрытии упаковки внутри обнаружен мобильный телефон марки «Samsung» в полимерном корпусе черного цвета. Телефон на момент осмотра находится в рабочем состоянии. Корпус телефона имеет потертости и загрязнение, что свидетельствует об эксплуатации мобильного телефона. При включении мобильного телефона было установлено, что в памяти телефона имеются различные мобильные приложения, в числе которых приложение для обмена сообщениями посредством сети Интернет – «Telegram».

При осмотре сохраненной переписки в приложении «Telegram» установлено, что имеются текстовые сообщения с временной отметкой 29 мая 2017 года, которые приведены на иллюстрациях № 5, 6, 7 в приложении № 1. После осмотра объект – мобильный телефон мар-

[1] Фрагмент протокола осмотра, предоставленного СУ УМВД России по Тверской области.

ки «Samsung» в полимерном корпусе серого и белого цветов, упакован в бумажный конверт коричневого цвета, опечатанный бумажной биркой с пояснительной надписью и подписью следователя, оттиском круглой печати «№ 7 СУ УМВД России по г. Курску»»[1].

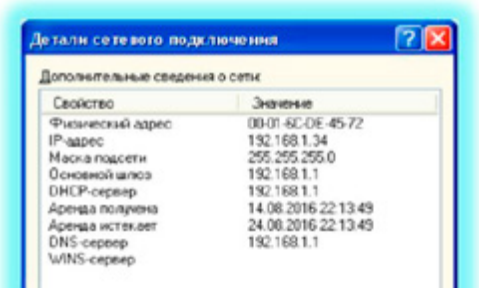
Анализ норм ст. 166, 177 и 180 УПК РФ позволил сделать вывод об отсутствии запрета на проведение осмотра электронного носителя информации перечисленными способами. В части 8 ст. 166 УПК РФ лишь упоминается о том, что к протоколу прилагаются фотографические негативы и снимки, киноленты, диапозитивы, фонограммы допроса, кассеты видеозаписи, чертежи, планы, схемы, слепки и оттиски следов, выполненные при производстве следственного действия, а также электронные носители информации, полученной или скопированной с других электронных носителей информации в ходе производства следственного действия.

Соответственно, выбор способа осмотра остается за следователем. Однако следует отметить, что первый способ является в настоящее время превалирующим в практической деятельности, так как затрачивает меньше времени при фиксации осмотра. При этом следует учитывать, что нетекстуальная часть протокола является приложением к нему и используется в доказывании как иной документ.

Наиболее целесообразным следует признать тактику осмотра, когда следователь указывает только путь к обнаруженной информации, а далее помещаются иллюстрации экрана устройства с информацией, представляющей значение для доказывания.

Например:

Вариант 1. «...Информация о MAC-адресе телефона была обнаружена следующим способом: «Menu» → «About phone» → «Status» → «MAC-адрес WI-FI» («Меню» → «Настройки» → «О телефоне» → «Техническая информация»)[2]».



[1] Фрагмент протокола осмотра, предоставленного СУ УМВД России по Курской области.

[2] Информация предоставлена ГСУ ГУ УМВД России по Саратовской области.

Вариант 2. «...При просмотре папки «Интернет» установлено, что в ней содержатся две папки «Prestigio» внутри которой находится файл «Интернет ресурсы», и «Ноутбук Asus», внутри которой, в свою очередь, находится папка «Браузеры», в которой находится файл «Браузеры_OverviewUrls».

Анализ файла «Браузеры_OverviewUrls» показал, что в нем в виде таблицы отображена информация о посещении интернет-ресурсов. Таблица представлена в виде колонок «Время последнего визита (местное)», «Время последнего визита (UTC)», «Ссылка», «Заголовок страницы», «Поисковый запрос», «Категория», «Путь происхождения», «Профиль». В таблице отображены сведения о посещении интернет-ресурсов за период с 29.04.2018 по 06.06.2018 по операторам сотовой связи, Банкам, денежным онлайн-переводам, Межрегиональный транзит телеком, интернет-почта, коды мобильных операторов, тарифные планы...»[1].

В соответствии с ч. 4 ст. 166 УПК РФ в протоколе должны быть описаны «выявленные при их производстве существенные для данного уголовного дела обстоятельства». В связи с этим следует признать не вполне оправданной практику фиксации всей без исключения информации, содержащейся на электронном носителе, которая была обнаружена следователем.

При этом в обязательном порядке в протоколе указываются условия и порядок использования устройств, с помощью которых изготавливаются копии изображения экрана (т. н. «скриншотов»). С указанной целью чаще всего используются встроенные функции операционной системы либо фотосъемка изображений на экране монитора.

Особенности осмотра и изъятия видеорегистратора. По конструктивным особенностям видеорегистраторы разделяются на три типа: а) моноблоки; б) устройства с откидным дисплеем; 3) приборы-зеркала. Моноблоки отличаются тем, что дисплей и объектив камеры находятся в одном блоке чаще всего прямоугольной формы. Второй тип более компактной формы, менее заметен. Самыми незаметными считаются видеорегистраторы в виде салонного зеркала заднего вида. Помимо явно установленных в салоне автомобиля (территории домовладения, квартиры, помещения) могут быть установлены закамуфлированные средства видеофиксации.

Следует учитывать, что запись на видеорегистратор происходит фрагментарно методом «каскада». При осмотре карты памяти,

[1] Фрагмент протокола осмотра, предоставленного СУ УМВД России по Курской области.

извлеченной из регистратора, можно обнаружить несколько файлов, которые перезаписываются по мере заполнения карты памяти. Карта памяти, изъятая с места дорожно-транспортного происшествия, может не содержать фрагмент записи, которая предшествовала ДТП, так как сохранение видеофайла остается незавершенным. При этом использование программного обеспечения, аппаратно-программных комплексов способствует восстановлению такой записи, что может стать неопровержимым доказательством, например нарушения ПДД.

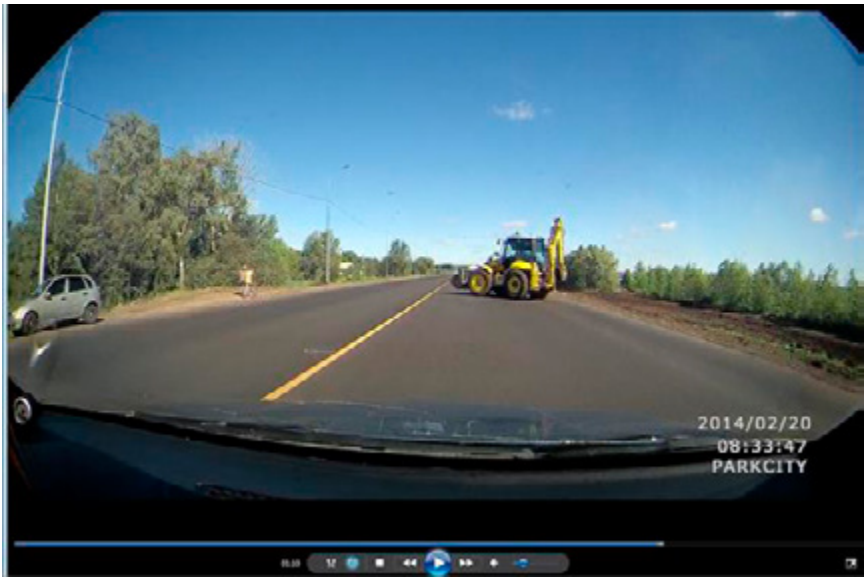
Пример: «...при осмотре видеорегистратора «PARKCITY» (712014020865) в слоте для карты памяти была обнаружена карта памяти «Transcend Micro SD» объемом 32 GB в черном полимерном корпусе, которая была извлечена из слота. На лицевой стороне имеется текст, выполненный красителем белого цвета, – «Transcend 32 GB Micro SD HC».

При осмотре электронного содержимого карты памяти (с помощью персонального компьютера) обнаружена папка «107MEDIA», при открытии которой были обнаружены 147 видеофайлов расширения (.MOV) именованные последовательно с «FILE4350.mov» до «FILE3596.mov».

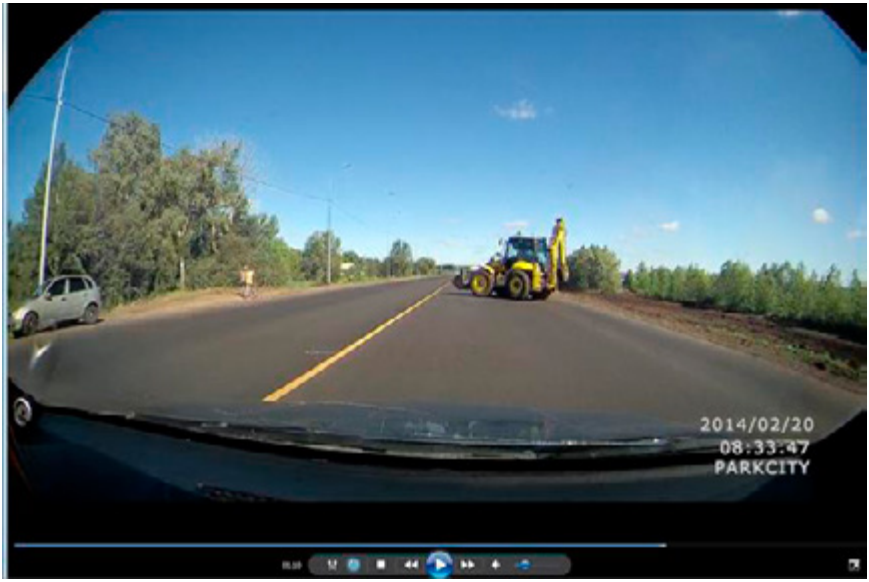
С целью восстановления несохраненных (непрописанных) в файловой системе карты памяти потоков данных (фрагментов несохраненных файлов видеорегистратора) перед экстренным выключением питания регистратора произведено восстановление файлов с помощью программ «Active FileRecovery 7.5.1» и «DMDE 3.0.4 Express Edition».

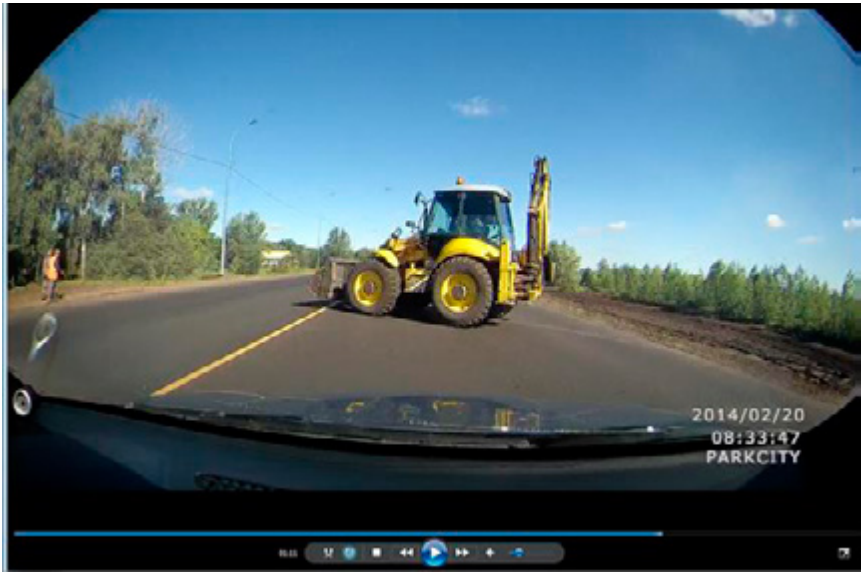
В целях отыскания поврежденных и скрытых файлов было использовано программное обеспечение, с помощью которого содержимое карты памяти Transcend 32 GB Micro SD HC было просканировано программами «Active FileRecovery 7.5.1» и «DMDE 3.0.4 Express Edition». В результате сканирования программами «Active FileRecovery 7.5.1» и «DMDE 3.0.4 Express Edition» поврежденных/скрытых (файлов, которые не отобразились в корневой папке «107MEDIA» при обычном просмотре, после того как флеш-карта – «Transcend 32 GB Micro SD HC» через кардридер была подсоединена к ПК) был обнаружен видеофайл – _ILE2776 (восстановленный), при открытии которого была обнаружена видеозапись, запечатленная непосредственно перед столкновением автомобиля «Шкода OCTAVIA TOUR», государственный регистрационный знак О 373 УУ 57 RUS, и экскаватора-погрузчика «NEW HOLLAND B115-B», государственный регистрационный знак 9269 77 RUS, произошедшем .... года на а/д «Орел-Там-

бов». При просмотре обнаруженного видеофайла установлено, что продолжительность видеозаписи _ILE2776 (восстановленный) составляет 01 минута 33 секунды, также установлено, что водитель автомобиля «Шкода OCTAVIA TOUR» государственный номер О 373 УУ 57 RUS Тимошкин С. Н. осуществляет движение по а/д «Орел-Тамбов» со стороны города Ливны в направлении города Орел ближе разделительной линии разметки.



На иллюстрации запечатлен момент маневра разворота экскаватора-погрузчика «NEW HOLLAND B115-B», государственный регистрационный знак 9269 77 RUS, под управлением водителя Большакова Е. В. (т. е. экскаватор-погрузчик начинает движение и перекрывает полосу движения), автомобиль «Шкода OCTAVIA TOUR», государственный регистрационный знак О 373 УУ 57 RUS, под управлением водителя Т. находился на дорожной метке «№ 3» (нанесенной на проезжей части автодороги «Орел – Тамбов») от места столкновения вышеуказанных транспортных средств. Данное расстояние (т. е. расстояние от места столкновения вышеуказанных транспортных средств до дорожной метки «№ 3», нанесенной на проезжей части автодороги «Орел-Тамбов») равно – 54.2 метра, т. е. для водителя Т. момент возникновения опасности для движения возник на расстоянии 54.2 метра.





После просмотра видеозаписи с учетом того, что данный видеофайл был скрыт и после его восстановления с карты памяти его необходимо перезаписать (т. е. сохранить) на электронный носитель в целях сохранности вышеуказанного видеофайла, на котором ото-

бражена дорожно-транспортная обстановка, возникшая непосредственном перед ДТП от .... года на а/д «Орел-Тамбов», видеофайл «_ILE2776 (восстановленный)» формата MOV с вышеуказанной видеозаписью ДТП от 22.06.2017 на а/д «Орел-Тамбов», с помощью ПК и привода DVD-ROM был записан на оптический диск DVD-R»[1].

При осмотре и изъятии видеорегистратора обязательно:

1. Фотографируется место, где был прикреплен корпус видеорегистратора (лобовое стекло автомобиля, стена подъезда, шлем и т. д.).

2. Изымаются не только карты памяти, но и корпусы видеорегистраторов, а также зарядные устройства (шнуры питания) к ним. При осмотре ДТП карты памяти не извлекаются из видеорегистраторов во избежание уничтожения имеющей значение информации для уголовного дела.

Рис. 2. Составные части видеорегистратора

Пример фиксации видеозаписи: Объектом осмотра является: конверт, выполненный из бумаги белого цвета, на котором имеется надпись, выполненная красителем черного цвета «Оптический диск, изъятый в ходе протокола от 03.10.2018, у свидетеля Шарова В. О.». При вскрытии бумажного пакета в нем обнаружен оптический диск с пояснительной надписью «intro DVD+R 120 min/4.7GB 1x-16x», выполненный из полимерного материала, окрашенный красителем бирюзового цвета.

[1] Фрагмент протокола осмотра, предоставленного СУ УМВД России по Орловской области.

После чего осматриваемый оптический диск с пояснительной надписью «intro DVD+R 120 min/4.7GB 1x-16x» был установлен в CD-Rom дисковод системного блока Intel (R) Pentium (R) 4 CPU 2.66 GHz 2.67 ГГц, 960 МБ ОЗУ, в результате чего и было установлено, что на нем содержатся файлы под названиями «1» и «2».

Файл под названием «1» при открытии самостоятельно распаковывается и производится воспроизведение видеофайла с помощью программы «Windows Media». В верхней правой части видеозаписи имеется дата – «2018-06-30» и время начала видеозаписи – «18.32.48». В левом нижнем углу имеется сведения о номере камеры «КАМ 13». На центральной части консоли программы «Windows Media» имеется также числовой маркер, который на момент начала видеозаписи обозначен «00:00».

При просмотре видеозаписи установлено, что на видеозаписи зафиксирован вид с наружной камеры, расположенной на стене капитального строения, которая производит видеосъемку проезжей части ул. Республиканская г. Курска и территорию, расположенную вдоль проезжей части ул. Республиканская г. Курска напротив д. 42-В по ул. Республиканская г. Курска. Согласно видеозаписи проезжая часть ул. Республиканская г. Курска представляет собой асфальтированное горизонтальное полотно, которое имеет 2 направления для движения. На данном участке проезжей части, согласно видеозаписи, имеется нерегулируемый пешеходный переход, который обозначен дорожными знаками «Пешеходный переход» и дорожной разметкой «Зебра». Видеозапись производится в светлое время суток.

Согласно временного / числового маркера «2018-06-30» «18.35.33» времени видеозаписи, а когда на центральной части консоли программы «Windows Media» числовой маркер равен «02:43», видно, как на проезжую часть ул. Республиканская г. Курска вступает пешеход-мужчина с сумкой в руках и начинает движение спокойным темпом шага справа налево по ходу движения автомобилей, по проезжей части ул. Республиканская г. Курска в направлении ул. 2-я Рабочая г. Курска. Пешеход вступил на проезжую часть с тротуара и начал движение по нерегулируемому пешеходному переходу по краю дорожной разметки «Зебра».

Согласно временного / числового маркера «2018-06-30» «18.35.39» времени видеозаписи, а когда на центральной части консоли программы «Windows Media» числовой маркер равен «02:50» видно, как на двигающегося по нерегулируемому пешеходному переходу пешехода допускает наезд легковой автомобиль, который осуществлял движение по проезжей части ул. Республиканская г. Курска в направлении ул. 2-я Рабочая г. Курска по левой полосе движения...

После проведения осмотра оптический диск с пояснительной надписью «intro DVD+R 120 min/4.7GB 1x-16x» извлечен из CD-Rom дисковода системного блока, помещен в конверт, опечатан, скреплен подписью следователя...[1]».

Тактика осмотра мобильного устройства мобильного телефона, смартфона, планшета. В условиях повсеместного использования мобильных телефонов (смартфонов) фигурантами следует учитывать ряд особенностей их работы, а также проблемы, связанные с извлечением данных из таких электронных носителей информации.

Поэтому осмотр следует начинать с определения состояния мобильного устройства. Наиболее благоприятными для проведения осмотра являются условия, когда устройство включено и разблокировано либо функция блокировки не включена, так как следователь получает полный доступ к информации на устройстве. При проведении осмотра в таких условиях следует незамедлительно:

А) включить «Режим полета». Определенной тактической проблемой является наличие удаленного доступа лица к информации, содержащейся на изъятых ЭНИ, что влечет возможность уничтожения значимой информации уже после их изъятия (например электронная переписка лица или иные данные, содержащиеся на сервере, местонахождение которого не было установлено)[2]. При активации режима «полет» отключаются все функции, способные принимать или передавать сигнал: сотовая связь, Wi-Fi, Bluetooth, GPS. При этом устройство продолжает функционировать как стандартное компьютерное устройство с операционной системой, приложения, не связанные с передачей или приемом данных, доступны для осмотра.

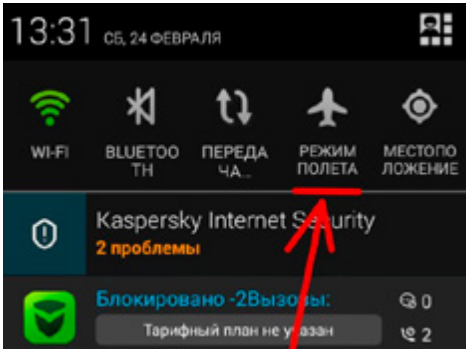


Рис. 3. Типичное графическое обозначение «Режим полета» в мобильном устройстве

[1] СУ УМВД России по г. Курску.

[2] Письмо ГСУ ГУ МВД России по Красноярскому краю от 25.07.2019 № 4/9492.

Это необходимо для того, чтобы фигуранты либо их подельники, родственники не могли воспользоваться сервисами:

– «Поиск телефона», который разработан кампанией Google для определения местоположения устройства с операционной системой Android в случае его утери либо хищения.

– «Найти iPhone», разработанный кампанией Apple для поиска смартфонов, нетбуков, ноутбуков, планшетов, смарт-часов, плееров с операционной системой iOS.

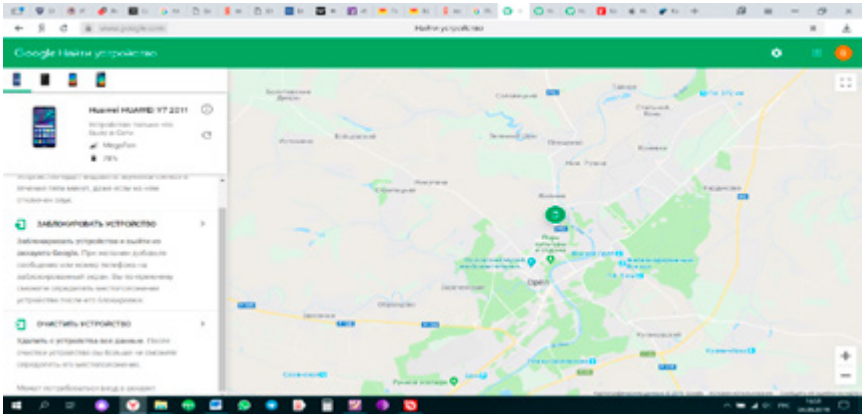


Рис. 4. Изображение экрана компьютера, с которого был получен доступ к устройству

С помощью любого компьютерного устройства, имеющего доступ к сети Интернет, пользователь имеет возможность благодаря указанным сервисам получить удаленный доступ к изъятому устройству. При этом фигурант имеет возможность удалить все данные из устройства, а также заблокировать его. В таком случае сведения на таком устройстве восстановить невозможно.

Следственной практике СУ СК РФ по Воронежской области известен случай, когда при проведении следственных действий в жилище подозреваемого следователь изъял смартфон и упаковал его без включения «полетного» режима. После чего выяснилось, что подельники фигуранта смогли удаленно стереть информацию с его смартфона.

Б) отключить блокировку экрана либо не допустить блокирование экрана устройства. Отключить блокировку при проведении осмотра мобильных устройств последних модификаций без участия пользователя практически невозможно. Поэтому особое значение имеет информация, которая может быть получена при проведении ОРМ в отношении интересующих лиц о паролях доступа к устройству.

В настоящее время существует несколько видов блокировки экрана мобильных устройств:

– *графический ключ*, который разблокирует экран устройства с помощью приложенного пальца к экрану по заданному шаблону в поле с девятью условными точками. Согласно шаблону необходимо провести пальцем от 4 до 9 точек, что дает больше миллионов возможных комбинаций;

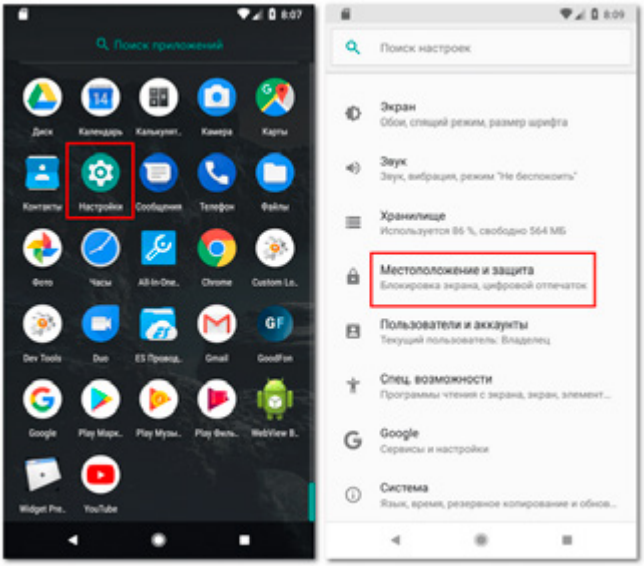
– *ввод PIN-кода* является наиболее распространенной разновидностью блокировки, выраженной в комбинации цифр;

– *сканирование радужной оболочки глаза,* является разновидностью системы биометрической системы распознавания пользователя. При сканировании используется специальный модуль и светодиод, освещающий лицо инфракрасным светом;

– *отпечаток пальца,* позволяет использовать только пальцы рук для разблокировки;

– *умная блокировка (Smart Lock),* позволяет не разблокировать устройство пользователю в случае: нахождения устройства рядом с телом (когда находится в определенном месте); нахождения в пределах досягаемости устройства Bluetooth; определения лица пользователя или голосовой команды (лицевая и голосовая биометрия).

В случае содействия фигуранта при проведении следственных действий следует выяснить вид блокировки, разблокировать устройство и отключить блокировку, после чего приступать к общему порядку осмотра устройства.



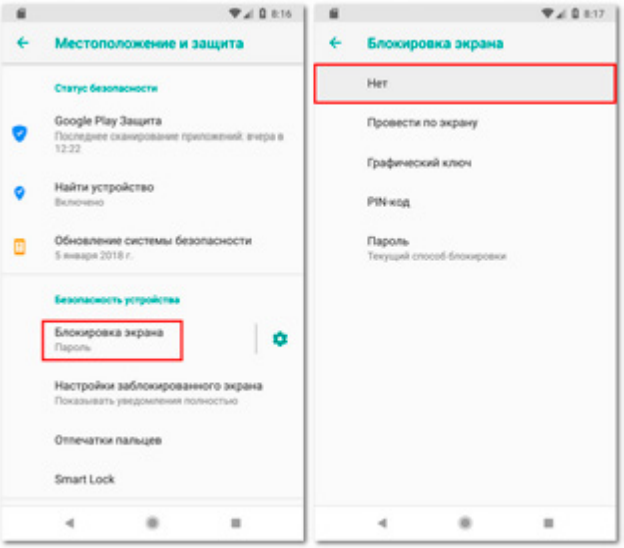


Рис. 5. Вариант отключения экрана блокировки

В случае формирования ситуации, когда подозреваемым не оказывается содействие, пароль неизвестен, заблокированное (сломанное) мобильное устройство осматривается в общем порядке (осмотр корпуса), упаковывается, изымается.

При этом решением возникшей проблемы может стать использование учетных записей пользователя для копирования данных из «облачного» хранилища. Так, допуск к «облаку» можно получить при проведении компьютерной экспертизы стационарного компьютера (ноутбука) фигуранта, который был обнаружен и изъят при обыске его жилища.

Вместе с тем, по информации, поступившей из ГСУ ГУ МВД России по Красноярскому краю, сотрудники органов предварительного следствия края сталкиваются с проблемами в виде противодействия фигурантов надлежащему изъятию электронных носителей информации, выражающегося в высокой степени защищенности информации, использовании удаленных «облачных» хранилищ. Однако, как правило, защита в виде использования паролей (при нежелании фигурантов сообщать их) преодолевается экспертами при проведении судебной компьютерной экспертизы. В ходе ее производства также восстанавливается вся удаленная информация с ЭНИ[1].

[1] Письмо ГСУ ГУ МВД России по Красноярскому краю от 25.07.2019 № 4/9492.

«Облако» часто содержит информацию о важных связях, которые помогают раскрывать преступления. Тем не менее доступ к облачному хранилищу часто отраничен. Например, GoogleDrive – популярное «облачное» хранилище, в котором пользователи хранят файлы и документы, а приложения, работающии в телефонах под управлением ОС Android, могут сохранять собственные данные и резервные копии (такие как резервные копии WhatsApp). Для входа в GoogleDrive может использоваться как стандартный способ с вводом логина и пароля, так и маркер аутентификации, извлеченный из браузера GoogleChrome специализированным программным обеспечением, что позволяет обойти дополнительную защиту по методу двухфакторной аутентификации.

В системе Apple, включающей компьютеры под управлением macOS, смартфоны iPhone, планшеты iPad и телевизионные приставки Apple TV, существует и активно используется механизм резервного копирования и синхронизации пользовательских данных посредством «облачного» сервиса iCloud. Если резервные копии iPhone или iPad создаются ежедневно во время зарядки, то синхронизированные данные попадают в «облако» практически без задержки. Синхронизируются такие данные, как закладки и история посещений веб-браузера Safari, список звонков и контактов пользователя заметки, пароли и многие другие данные. Извлечение синхронизированных данных позволяет собрать огромный массив информации о пользователе, его «абонентском» поведении и привычках даже в случаях, когда создание резервных копий в iCloud запрещено. Дистанционное извлечение данных из iCloud доступно как при наличии логина (Apple ID) и пароля пользователя, так и без них с использованием вместо пароля маркера аутентификации, извлеченного из компьютера пользователя. Доступ к самому устройству при этом не требуется.

Кроме того, экспертами используется программное обеспечение, позволяющее эмулировать работу целой операционной системы, – виртуальная машина. Это означает, к примеру, что пользователь может иметь как бы второй Windows-компьютер, обозначаемый как «гость», который хранится на компьютере, обозначаемый как «хозяин». Большинство виртуальных машин позволяет шифровать файлы, находящиеся на жестком диске виртуальной машины. Это означает, что виртуальная машина не может быть активирована без соответствующего пароля. При таких обстоятельствах можно использовать защищенную паролем виртуальную машину для всех операций с виртуальными валютами, при этом не оставляя никаких

следов использования виртуальных валют в основной операционной системе, обозначаемой как «хозяин».

Анализ данных сетевого (входящего и исходящего) трафика компьютера подозреваемого осложнен рядом трудностей, способных осложнить сбор доказательств. Во-первых, канал связи между компьютером подозреваемого и компьютером, с которым он находится в контакте, скорее всего, будет зашифрован. Во-вторых, существуют онлайновые возможности, позволяющие пользователям скрывать тот факт, что они участвуют в коммуникации. Речь идет о специальных прокси-программах, позволяющих установить анонимное сетевое соединение. Их существует несколько видов, из которых самая известная – Tor, ранее известная как «TheOnionRouter». Tor осуществляет шифрование и передачу трафика через серию промежуточных узлов. Трафик, проходящий через систему Tor, представляется другим серверам в сети Интернет как таковой, который будто бы берет начало из какой-то условной точки, а не из истинного источника (то есть компьютера подозреваемого). Отследить трафик и выйти на истинный источник чрезвычайно трудно[1].

Также обойти двухфакторную аутентификацию, если она активирована, можно получением SMS-сообщения на SIM-карту, извлеченную из того же мобильного устройства.

В условиях, когда мобильное устройство удалось изъять в разблокированном состоянии, но блокировку экрана отключить не получилось, следует незамедлительно инициировать проведение исследования устройства с помощью аппаратно-программных комплексов специалистом.

Если же такой возможности нет, то в кратчайшие сроки необходимо зафиксировать информацию, которая представляет значение для уголовного дела, с помощью детальной фотосъемки экрана мобильного устройства. В свою очередь, необходимо предпринять меры по недопущению блокировки экрана (регулярное касание рукой экрана либо пролистывание).

Как отмечается в информации, поступившей из ГСУ ГУ МВД России по г. Санкт-Петербургу и Ленинградской области, к тактическим проблемам собирания доказательственной информации в компьютерных сетях, устройствах сотовой телефонной связи, автономных микропроцессорных устройствах и иных электронных носителях относятся отсутствие программных и технических средств раскодирования и расшифрования полученных в ходе следственных действий электронных данных, хранящихся на изъятых

[1] Письмо СУ УМВД России по Брянской области от 22.07.2019 № 17/8587.

носителях информации, а также отсутствие возможности эффективного обнаружения и изъятия информации, хранящейся на виртуальных серверах, размещенных, в том числе, и на территории других государств[1].

При проведении осмотров (обысков) в офисных помещениях, где фигурантами используются большое количество мобильных устройств, следует обращать внимание на записи, сделанные в тетрадях, на офисных стикерах, записках. На них могут быть оставлены сведения о паролях к экранам мобильных устройств, другим электронным носителям информации.

После определения состояния мобильного устройства и принятия экстренных мер по сохранению и фиксации информации следует уделить внимание осмотру основных признаков мобильного устройства. К таким признакам относятся:

1. Идентификационный номер устройства IMEI. Как правило, IMEI указывается в четырех местах:

– в самом аппарате (в большинстве случаев его можно вывести на экран набором *#06# на клавиатуре);

– на задней панели корпуса устройства (iPhone, HTC, Google Nexus и др.);

– под аккумуляторной батареей;

– на упаковке;

– в гарантийном талоне.

IMEI играет роль серийного номера аппарата и передается в эфир при авторизации в сети. Для просмотра IMEI специалист и/или следователь могут воспользоваться следующим алгоритмом управления меню: «настройки» – «об аппарате» – «общая информация». Следует учитывать, что номера IMEI могут повторяться у так называемых «серых» телефонов. «Серые» телефоны можно поделить на контрафактные и подделки. Контрафактные производятся на официальных заводах, но ввозятся в Россию нелегально, а подделки производятся кустарным способом, хотя внешне они очень похожи на оригиналы. При этом следует обратить внимание на признаки грубой подделки сотовых телефонов (например ошибки в написании известных моделей телефонов) и при их наличии отразить это в протоколе[2].

[1] Письмо ГСУ ГУ МВД России по г. Санкт-Петербургу и Ленинградской области от 06.08.2019 № 8/22989.

[2] *Земцова С.И.* Методика расследования незаконного сбыта наркотических средств, совершенного с использованием интернет-технологий: учебное пособие / С.И. Земцова, О.А. Суров, П.В. Галушин. Москва: Юрлитинформ, 2019.

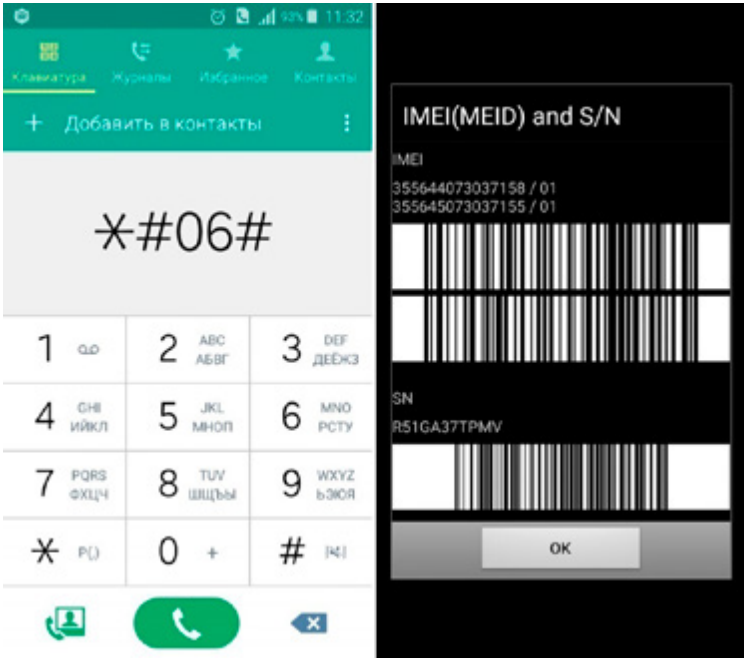


Рис. 6. Определение IMEI с помощью команды с клавиатуры

Рис. 7. IMEI, нанесенный на держателе SIM-карты сотового телефона

Необходимо иметь в виду, что может быть произведена смена IMEI для создания двух или нескольких телефонов, одинаково

опознаваемых сетями сотовой связи, что позволяет преступникам «размывать» информацию о своем местонахождении.

2. Установочная информация о мобильном устройстве (модель устройства), операционная система, версия прошивки, телефонный номер SIM-карты, IP-адреса, MAC-адреса. Данная информация содержится в приложении «Настройки» при нажатии значков «Об аппарате», «Общая информация».

В случае если владелец мобильного устройства отказывается предоставлять информацию о паролях мобильного телефона, а следователю или специалисту в ходе проведения следственного действия установить их не удалось, то осмотр мобильного телефона и SIM-карты будет только внешним. Такой осмотр необходим для идентификации устройства, SIM-карты, карты памяти и последующего их направления на судебную компьютерную экспертизу.

Наиболее типичными упущениями при фиксации осмотра и изъятия ЭНИ является отсутствие в протоколах следственных действий указаний на конкретную марку используемых специалистом технических средств и описания проведенных им манипуляций[1].

3. Электронные данные мобильного устройства. Значительную часть данных в мобильном устройстве занимает приложение «Контакты», в котором содержатся внесенные пользователем телефонные номера, фотографии и краткие сведения об их владельцах. Осмотр данной информации позволяет установить круг общения пользователя мобильного телефона, его интересы, место работы.

В приложении «Журнал вызовов» мобильного устройства отображаются принятые, непринятые, исходящие телефонные вызовы в виде номеров. Изучение данного раздела дает общее представление о количестве, повторяемости последних местных или междугородних звонков (как правило, тактический эффект; однако эти сведения могут быть положены в основу доказывания ряда составов преступлений, где значение имеет факт общения определенных лиц друг с другом: бандитизм, организация преступного сообщества или участие в нем и пр.). При описании в протоколе осмотра исходящих и входящих телефонных номеров следует обращать внимание на дату, время начала и продолжительность соединения пользователя мобильного телефона с номером конкретного абонента.

Приложение «Сообщения» содержит сведения о входящих, исходящих SMS, MMS, EMS, голосовых сообщениях и отчет о доставке таких сообщений. Принятые и отправленные сообщения могут содержать текст, иллюстрации, фотографии, звукозаписи. В протоколе следствен-

[1] Письмо ГСУ ГУ МВД России по Московской области от 08.08.2019 № 14/7993.

ного действия отображаются сведения о SMS-, EMS-, MMS-сообщениях и их дословное содержание (для текстов). Сведения о SMS-, EMS-, MMS-сообщения включают номер, на который они отправлены и с которого они получены, дата и время отправления и получения сообщения.

При изучении указанных приложений в памяти телефона на SIM-карте, в облачном хранилище (на сайте), на карте памяти можно установить не только перечень абонентов, с которыми осуществлялось общение, но и выявить дополнительную информацию: фотографии контактов, адреса электронной почты, группы, почтовые адреса, псевдонимы, дни рождения, регистрацию контактов в интернет-мессенджерах, профили в социальных сетях и другое.

Для быстрого создания копии списка контактов, например в ОС Android, специалист, участвующий в осмотре, может подключить телефон к стационарному компьютеру и при необходимости инсталлировать предлагаемую телефоном программу синхронизации, после чего сохранить контакты на компьютере и распечатать на бумажный носитель, отразив данную операцию в протоколе.

Как показывает изучение материалов уголовных дел, предоставленных территориальными органами при осмотре мобильных устройств следователями, недостаточное внимание уделяется сведениям, которые сохраняются в устройстве по умолчанию. К таким сведениям относятся:

– *хронология маршрутов Google Карты,* которая позволяет просмотреть историю местоположения аккаунта, которым пользуется фигурант за последние годы, месяцы, дни. Данные сведения доступны в случае включенного датчика GPS либо сети WI-FI во время передвижения устройства.

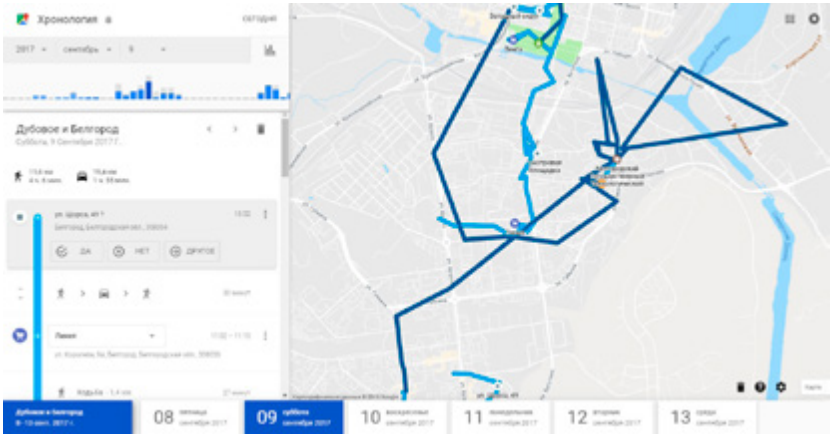


Рис. 8. Хронология передвижения и посещения определенных мест мобильного устройства, выведенная с помощью подключения к аккаунту компьютера

Если в осматриваемом устройстве включена история приложений и веб-поиска, геоданные сохраняются в аккаунте при использовании других сайтов, приложений и сервисов Google. Например, при включенной истории приложений и веб-поиска данные о местоположении могут сохраняться в результате действий в Google Поиске и на Картах, а также в зависимости от настроек камеры добавляться в сведения о фото;

– *геопозиционные данные фотографий, сделанных с помощью мобильных устройств,* которые можно обнаружить в свойствах осматриваемых фотографий. Данные сведения доступны в случае включенного датчика GPS в момент изготовления фотографии.

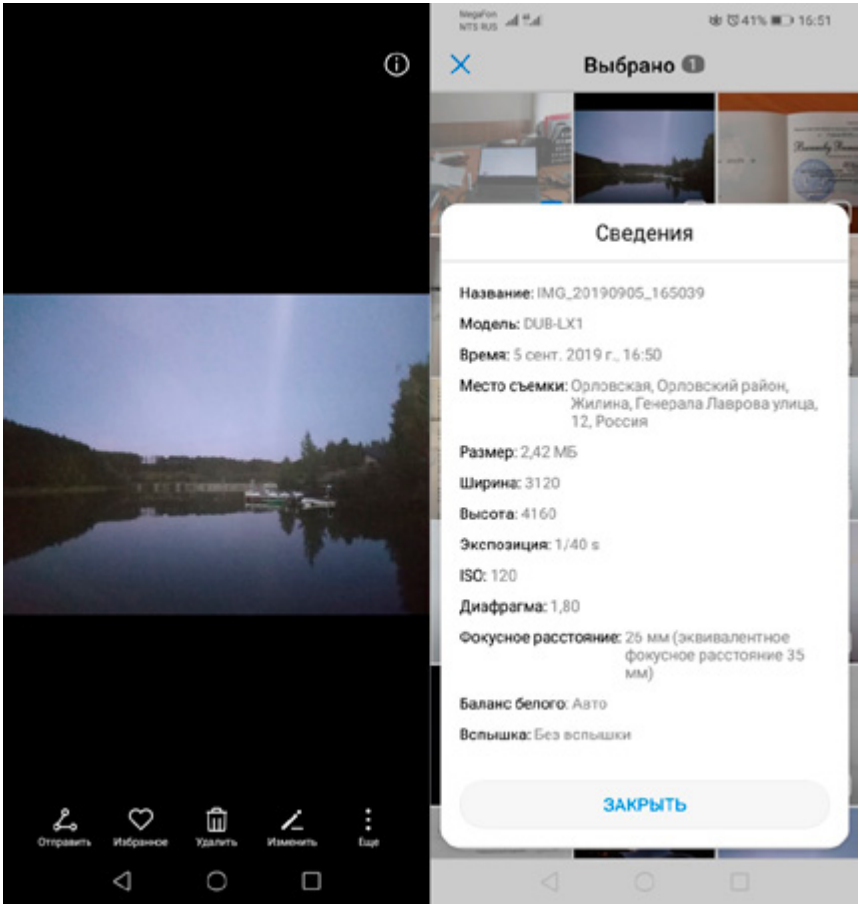


Рис. 9. Вид фотографии и сведений о ней, которые содержатся в мобильном устройстве

4. Электронные данные браузера. При осмотре следует особое внимание обращать на веб-браузеры (Google Chrome, Android Browser, Opera, Яндекс.Браузер и др.), установленные на мобильном устройстве, а также историю просмотра веб-страниц и закладок в браузере.

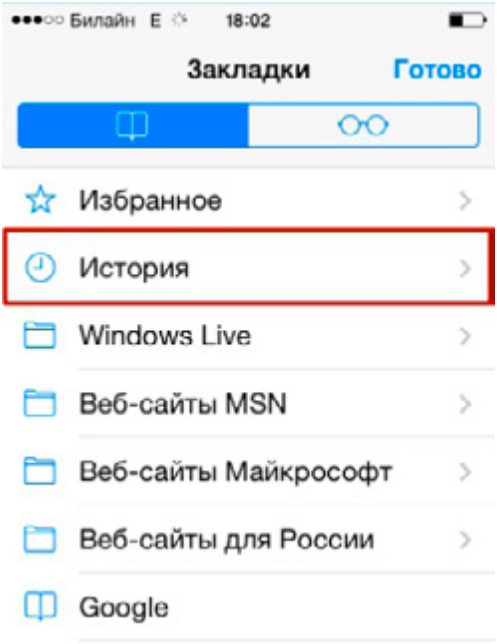


Рис. 10. Вид значка «История» в браузере мобильного устройства

Детальному анализу должны быть подвергнуты:

– информация о социальных сетях («ВКонтакте», «Facebook», «Одноклассники» и т. д.), а также форумы, посредством которых происходило общение;

– информация с различных сайтов, которые посещал фигурант.

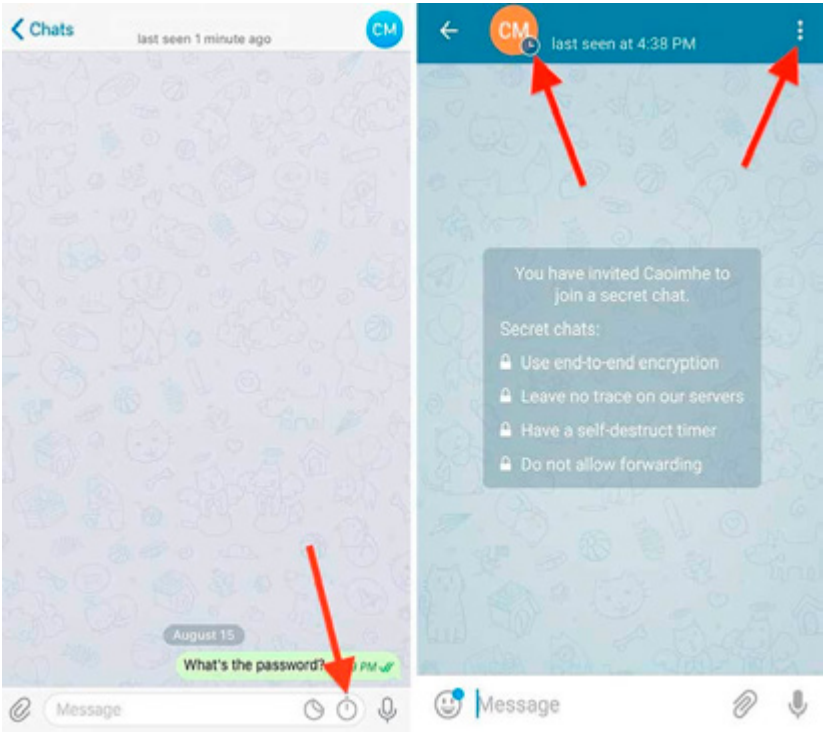
5. Изучение приложений-мессенджеров. Чаще всего абонентская активность фигурантов проявляется при общении с помощью мессенджеров (WhatsApp, Viber, Brosix, Telegram и др.). Ключевое значение для доказывания, как правило, имеют сведения:

– о контактах, которые осуществляются с помощью чатов, а также аудио- и видеозвонков;

– о содержании обмена тестовой, символьной, аудио- и видеоинформации между фигурантами.

Особую популярность среди подозреваемых приобрел мессенджер Telegram в связи с нахождением его серверов за пределами Российской Федерации, что повышает конспиративность фигурантов.

Также использование Telegram обусловлено встроенной функцией «секретных чатов», которые обеспечивают полную анонимность пользователей, а также возможность прикреплять к сообщениям «таймер самоуничтожения» и очищать «историю сообщений» удаленно – через другие устройства. Технические возможности программы Telegram предъявляют дополнительные требования к фиксации информации в ходе осмотра. Для предотвращения уничтожения переписки в контролируемом при следственном действии чате необходимо изменить настройки – закладка – Set self-destruct timer – с периода времени на off [1];



[1] *Земцова С. И.* Методика расследования незаконного сбыта наркотических средств, совершенного с использованием интернет-технологий: учебное пособие. Москва: Юрлитинформ, 2019.

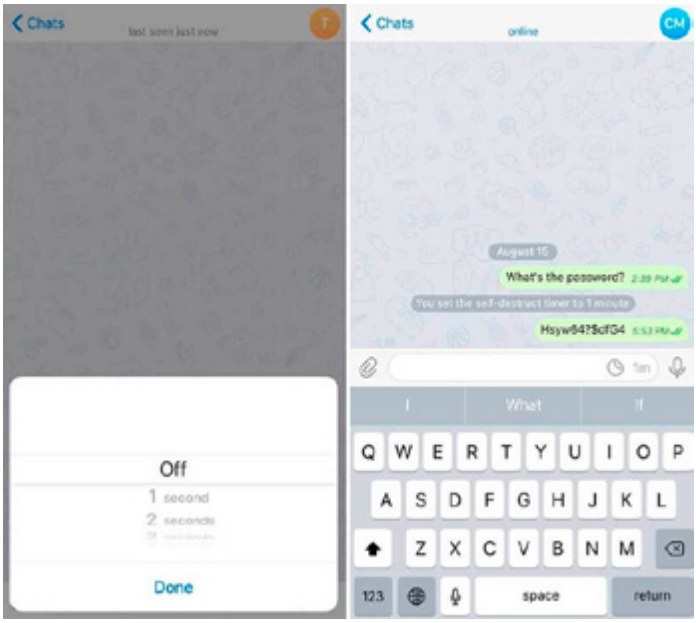


Рис. 11. Алгоритм отключения таймера в секретном чате Telegram

– о фотографиях, отражающих отдельные факты преступной деятельности (например мест тайников и закладок, внешнего вида наркотического средства и т. д.);

Рис. 12. Вид переданной фотографии в приложении Telegram

Пример описания: *«Объектом осмотра № 2 является папка «ZTEBladeX3 T620», при открытии которой обнаружена 1 папка «Telegram», а также 6 документов Excel – «GoogleChrome», «ВКонтакте», «Лента событий», «Объединенные контакты», «Сообщения», «Телефонная книга». Осмотр папки «Telegram» показал, что в указанной папке имеются две папки - «org.telegram.messender», «Telegram», а также документ Excel с наименованием «Telegram». Открыв папку «org.telegram.messender», установлено, что в указанной папке находится папка «cache», в которой имеется 2 111 фотофайлов, которые из-за маленького разрешения не читаемы. Открыв папку «Telegram», установлено, что в ней содержатся две папки с названиями «TelegramAudio» и «TelegramImages». При осмотре папки «TelegramImages» установлено, что в ней содержатся 896 фотофайлов, которые содержат информацию...»*[1];

– о видеофайлах (например совместного времяпрепровождения участников преступной группы, содержащих информацию о способах совершения преступления, и т. д.);

– о местоположении и маршруте движения согласно GPS/ГЛОНАСС (например по ходу движения транспортного средства до дорожно-транспортного происшествия);

– о наименовании сетей Wi-Fi, к которым телефон ранее подключался, в том числе стационарных (мест пребывания фигуранта, потерпевшего и других участников).

Применение средств поиска файлов. При производстве следственного действия нужно иметь в виду, что файлы могут находиться как в памяти телефона, так и на картах памяти. В протоколе осмотра следователю при оказании консультационной помощи специалиста необходимо отразить их производителя, объем и серийный номер карты, при наличии переключателя защиты от записи (замка) – его положение. После этого нужно включить защиту от записи, чтобы исключить модификацию данных, хранящихся на карте.

В некоторых случаях сохраненные файлы могут быть недоступны для просмотра средствами операционной системы мобильным устройством, поэтому целесообразно иметь переносной компьютер с USB-проводом, картридером и программами просмотра распространенных форматов файлов (doc, docx, pdf, djvu и т. д.), а также программами подбора паролей для различных типов файлов (например, Advanced Archive Password Recovery).

Контакты, SMS-сообщения и файлы в памяти телефона должны быть сохранены специалистом на внешних носителях с помощью

[1] Фрагмент протокола осмотра, предоставленного СУ УМВД по Тверской области.

соответствующего аппаратного и программного обеспечения. С этой целью может быть использована программа Мобильный Криминалист или программно-аппаратный комплекс UFED. Достоинством последнего являются более широкие возможности использования, позволяющие производить полное извлечение таких данных, как телефонная книга, текстовые сообщения, фотографии, видеоизображения, журналы звонков (исходящих, входящих, пропущенных), звуковые файлы, идентификационные данные телефона и т. д.[1]

Анализ норм, посвященных изъятию электронных носителей информации, позволяет выделить следующие формы возможного копирования при производстве следственного действия:

1) обеспечительная копия – изготавливается специалистом по ходатайству владельца носителя информации для недопущения нарушений должного функционирования юридического лица, предпринимательской деятельности физического лица. Данная форма копии переносится на электронный носитель, который предоставляется ходатайствующей стороной. При этом, если какая-либо информация представляет криминалистическую значимость для расследования, а доступ к ней может повлечь определенные меры противодействия со стороны владельца электронного носителя, передавать такую копию тактически не целесообразно.

Образец обозначения в протоколе процесса копирования.

...Изъятие данного документа без изъятия ноутбука невозможно, так как папка являлась системной. Ходатайство Петрова А. А. о копировании документа Microsoft Word размером 70 кб, созданного 20 марта 2015 года, «Итоги за март» было удовлетворено. Петровым А. А. был предоставлен флэш-носитель «Kingston» объемом 16 GB. После осуществления копирования флэш-носитель был передан заявителю. Замечаний по ходу и результатам копирования от Петрова А. А. не последовало... Подписи Петрова и специалиста;

2) протокольная копия – изготавливается специалистом в ходе проведения обыска (выемки) в целях получения доказательственной информации из электронного носителя, который в силу громоздкости или исключительной важности для ведения правомерной хозяйствующей деятельности организации не подлежит изъятию. Например, такими носителями могут стать серверы крупных компаний, операторов связи, кредитных организаций.

---

[1] *Земцова С. И.* Методика расследования незаконного сбыта наркотических средств, совершенного с использованием интернет-технологий: учебное пособие. Москва: Юрлитинформ, 2019.

В данном случае весь процесс копирования происходит в присутствии понятых, которым по мере необходимости специалист поясняет цель производимых манипуляций, а также их результаты. По завершению копирования электронный носитель, на который была перенесена копия, упаковывается и опечатывается.

Фиксация факта, хода, содержания и результатов обыска и выемки по уголовным делам, где фигурируют электронные носители, производится по общим правилам, установленным уголовно-процессуальным законодательством.

В любом случае составляется протокол с соблюдением требований, изложенных в ст. 166 УПК РФ. В протоколе фиксируются сведения об объектах, обнаруженных и изъятых в ходе обыска, выемки на электронных носителях, информации в электронной форме и иных объектов, дающих основания для выдвижения версий о наличии и месте нахождения названных носителей и информации.

В протоколе обыска, в отличие от протокола осмотра, отсутствует обязательность фиксации подробных сведений об изъятом объекте, так как в дальнейшем можно будет восполнить эти данные путем проведения осмотра предметов и документов. В остальном обнаруженные и изъятые объекты описываются по правилам, ранее обозначенным для осмотра.

Упаковка изымаемых электронных носителей информации должна исключать возможность непроцессуальной работы с ними, возникновение на них механических повреждений, разукомплектования, модификации находящейся на нем информации, а в конечном счете – обеспечивать достоверность полученной доказательственной информации. С указанной целью производится опечатывание клапанов упаковки таким образом, чтобы вскрытие было невозможно без повреждения опечатывающих наклеек. Сам электронный носитель помещается в экранирующую тару («мешок Фарадея»), который должен исключать возможность дистанционного считывания информации посредством удаленного доступа (синхронизации) устройств-«перехватчиков».

При составлении протокола следственного действия, в ходе которого появилась необходимость изъятия электронного носителя, следует обращать внимание на описание места расположения информации, наименование, метаданные изымаемых (скопированных) данных и (или) размерные характеристики (форм-фактор) электронного накопителя в случае, если он изымается вместе с хранящейся информацией. В литературе обоснованно отмечается возможное несоответствие применяемой терминологии следователем при обращении с электронными устройствами, которое может при-

вести к определенным трудностям при признании и приобщении их в качестве вещественных доказательств[1]. Так, например, по форме USB-флэш-накопители могут быть идентичны ключам электронной подписи, Bluetooth-устройствам, интернет-модемам. Между тем, функциональное назначение указанных устройств в корне отличается. Указанное обстоятельство еще раз свидетельствует о необходимости использования специальных знаний при проведении изъятия электронных носителей.

Дополнительно можно оформить схему обнаружения искомых (изъятых) объектов и приложить фотоснимки, в том числе сделанные с применением специальных сканирующих программ. При этом отсутствует необходимость в детальном вычерчивании всего места обыска (схем расположения средств компьютерной техники, каналов и средств связи, инженерно-технических коммуникаций и т. д.).

Вопросы для повторения

1. Раскройте сущность и назовите способы собирания доказательств.
2. Какие должностные лица вправе собирать доказательства.
3. Укажите тактические особенности процесса обнаружения доказательств на электронных носителях.
4. Раскройте тактические особенности фиксации и изъятия доказательств на электронных носителях.

Практические задание

Произвести описание представленного объекта (видеорегистратора, мобильного телефона, планшетного компьютера) в виде фрагмента протокола осмотра.

---

[1] *Грибунов О. П., Старичков М. В.* Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие. Иркутск: ФГКОУ ВПО ВСИ МВД России, 2014. С. 88, 89.

§ 2. Особенности проверки и оценки доказательственной информации на электронных носителях

Под проверкой доказательств в уголовном процессе понимается деятельность следователя и суда, связанная с анализом и синтезом доказательств, сопоставлением их с другими доказательствами и собиранием новых доказательств[1]. Целью проверки доказательств, по мнению ряда авторов, является уяснение качеств и свойств самих проверяемых доказательств – их достоверности или недостоверности, правильности или неправильности, доброкачественности[2].

Проверка доказательств осуществляется путем их сопоставления, установления источника доказательства, а также посредством производства следственных и иных процессуальных действий, в ходе которых получаются новые доказательства, которые, в свою очередь, сопоставляются с проверяемым доказательством. В ходе проверки исследуются все обозначенные свойства доказательств и источник их происхождения, устанавливается достоверность содержащихся в доказательствах сведений.

Ни одно доказательство, каким бы убедительным и безупречным оно ни казалось, не может быть положено в основу выводов по уголовному делу без их проверки[3]. Проверке подвергается как содержание доказательства, так и доброкачественность источника его получения в их неразрывном единстве. При этом нарушение указанных правил повлечет за собой тот факт, что доказательство, полученное с нарушением основных положений судопроизводства, хотя и не носящим преступного характера, – недопустимо. Иначе говоря, в таких случаях доказательства просто не существует, поскольку сведение не обладает свойством допустимости.

---

[1] *Строгович М. С.* Курс советского уголовного процесса. Москва, 1958. С. 163–164; *Он же*. Теория доказательств в советском уголовном процессе. Москва: Юр. лит., 1966–1967: в 2-х т. С. 301–302; *Трусов А. И.* Основы теории судебных доказательств. Москва: Госюриздат, 1960. С. 84.

[2] *Арсеньев В. Д.* Вопросы общей теории судебных доказательств. Москва, 1964. С. 15–16; *Белкин Р. С.* Собирание, исследование и оценка доказательств. Сущность и методы. Москва, 1966. С. 48–49, 59; *Строгович М. С.* Курс советского уголовного процесса. Москва, 1958. С. 303; *Он же*. Теория доказательств в советском уголовном процессе. Москва: Юр. лит, 1966–1967: в 2-х т. С. 302.

[3] При производстве по уголовному делу, осуществляемому в порядке дознания в сокращенной форме (гл. 32.1 УПК РФ), законодатель позволяет дознавателю не проверять доказательства, если они не оспариваются потерпевшим, его представителем, подозреваемым, его защитником (п. 1 ч. 3 ст. 226.5 УПК РФ). Это решение основано не на познавательных закономерностях, которые обеспечивают систему элементов процесса доказывания – собирание, проверка и оценка доказательств.

При проверке доказательств должны учитываться особенности источника информации (в данном случае речь идет о материальном источнике доказательств), обстоятельства и условия формирования доказательства, обстановка, в которой были обнаружены сведения.

Формы проверки доказательств представляют собой либо мыслительные операции (сопоставление полученного доказательства с уже имеющимися), либо практическую деятельность (установление источников доказательств; получение иных доказательств).

Законодатель не раскрывает, что следует понимать под установлением источников доказательств. Однако, судя по контексту, установление источников доказательств представляет собой установление особенностей материального носителя информации либо характеристик лица, предоставившего информацию.

Проверка доказательств посредством получения новых доказательств проводится в двух вариантах. Во-первых, новые доказательства могут свидетельствовать о наличии (отсутствии) устанавливаемого факта и тем самым подтверждать (опровергать) уже имеющиеся доказательства. Во-вторых, новые доказательства могут устанавливать обстоятельства, знание которых необходимо для правильной оценки имеющихся доказательств (в частности, при установлении материального источника информации, знание о котором необходимо для оценки полученного от него сведения). Получение новых доказательств с целью проверки уже имеющихся является не чем иным, как собиранием доказательств. «Проверка доказательств, – пишет Ю. К. Орлов, – является таковой только в отношении проверяемых доказательств, для проверяющих она выступает как собирание»[1].

Оценка доказательств производится на предмет их относимости, допустимости, достоверности, а всей совокупности имеющихся доказательств – на предмет достаточности (ст. 88 УПК РФ).

Оценка доказательств, в отличие от проверки, – деятельность исключительно мыслительная, а не практическая и осуществляется по внутреннему убеждению должностных лиц, основанному на совокупности имеющихся в уголовном деле доказательств, руководствуясь при этом законом и совестью. Ни одно доказательство не имеет заранее установленной силы (ст. 17 УПК РФ).

Оценка доказательств по внутреннему убеждению – одно из самых великих достижений в развитии уголовно-процессуального законодательства в мире. В Россию это достижение пришло в 1964 г. в виде положений Устава уголовного судопроизводства

[1] *Орлов Ю. К.* Основы теории доказательств в уголовном процессе: научно-практическое пособие. Москва: Проспект, 2000. С. 78.

о свободной оценке доказательств. До принятия указанного Устава доказательства в России оценивались по формальным правилам, когда их сила определялась нормативными актами.

Сегодня в литературе высказывается мнение, согласно которому формальные правила при оценке доказательств следует оценивать положительно, а законодательство развивается в сторону легализации этих формальных правил[1].

Согласно ст. 17 УПК РФ при оценке доказательств действительно следует руководствоваться законом и совестью. Действительно ли закон исключает формальную составляющую, если сам же законодатель требует руководствоваться при оценке доказательств законом? Мало того, в УПК РФ содержится ряд положений, связанных с оценкой доказательств. Например, это основания признания доказательств недопустимыми (п. 1, 2 ч. 2 ст. 75 УПК РФ), преюдиция (ст. 90 УПК РФ), случаи обязательного назначения и производства судебной экспертизы (ст. 196 УПК РФ) и др.

Между тем, указанные правила не затрагивают собственно оценку доказательств, хотя и оказывают на нее влияние. Оценка доказательств – мыслительная деятельность, которая не может быть предметом правового регулирования и осуществляется по закономерностям, законодателю неподвластным. Правила, установленные законодателем, могут предопределить лишь совокупность той доказательственной базы, которая подлежит оценке должностными лицами, осуществляющими производство по уголовному делу, но не предопределяют преимущества одних доказательств перед другими. Даже в случаях обязательного назначения экспертизы (ст. 196 УПК РФ) законодатель требует, чтобы в совокупность доказательств, подлежащих оценке, было включено заключение эксперта, а не устанавливает его преимущество перед другими доказательствами[2].

Требование руководствоваться при оценке доказательств совестью высвечивает нравственный характер уголовного судопроизводства, его доказательственной деятельности и выступает одной из гарантий добросовестности должностных лиц, его осуществляющих. Совесть как процессуальная гарантия служит не процессу оценки доказательств, а процессу оценки его итогов. Правоприменитель должен не сомневаться, что относимость,

[1] *Зотов Д. В., Сыщикова Т. М.* Быть по сему!? // Судебная власть и уголовный процесс. Научно-практический журнал. 2014. № 3. С. 168.

[2] См. об этом: *Победкин А. В.* Принцип свободы оценки доказательств и его влияние на законность досудебного производства // Труды Академии управления МВД России. 2017. № 1. С. 104–108.

допустимость, достоверность и достаточность доказательств определена правильно[1].

Проведенные опросы сотрудников органов предварительного следствия и дознания системы МВД России показали, что практические сотрудники испытывают затруднения с оценкой доказательств на электронных носителях.

Раскроем особенности проверки и оценки относимости, допустимости, достаточности и достоверности доказательственной информации, содержащейся на электронных носителях, для возможности ее использования в ходе производства по уголовным делам.

Относимость доказательства означает его пригодность устанавливать факты, являющиеся предметом доказывания, определять логическую связь между сведениями, которые составляют содержание доказательства, и тем, что нужно установить для правильного разрешения уголовного дела. Доказательство относимо, если между сведениями об обстоятельствах и самими обстоятельствами, подлежащими доказыванию, существует связь, позволяющая использовать сведения для установления указанных обстоятельств. Относящимся к делу признается лишь то доказательство, которое прямо или косвенно подтверждает какие-либо из обстоятельств, имеющих значение для уголовного дела[2] (ст. 73 УПК РФ и другие его положения, предусматривающие основания для принятия различных уголовно-процессуальных решений).

Л. Д. Кокорев и Н. П. Кузнецов верно подчеркивают, что в ходе расследования представление об относимости может меняться: перестанет считаться относящимся к делу то, что ранее признавалось таковым. Результат может быть и противоположным, поскольку то, чему следователь первоначально не придал значения, в дальнейшем окажется в действительности весьма важным[3]. Это, конечно, не свидетельствует о том, что информация изменила свое значение. Меняется сама оценка сведений по мере того, как вероятное становится достоверным. Относимость же доказательства всегда объективна: связь между сведением и доказываемым обстоятельством либо есть, либо нет.

В вопросе допустимости доказательств на сегодняшний день существуют спорные вопросы, что связано с сущностью допустимости, которую понимают по-разному. Для формирования доказательств

---

[1] *Там же.*

[2] *Кореневский Ю. В., Падва Г. П.* Участие защитника в доказывании по новому уголовно-процессуальному законодательству. Москва, 2004. С. 19.

[3] *Кокорев Л. Д., Кузнецов Н. П.* Указ. соч. С. 125.

первичным материалом служат сведения, которые сами по себе доказательствами не являются. Форма сохранения этих сведений зависит от источников доказательства. Сведение приобретает свойство допустимости, т. е. становится доказательством только в том случае, если в установленном законом порядке приобрело форму одного из источников доказательства. В этом смысле, невзирая на наименование ст. 75 УК РФ, недопустимых доказательств не существует.

В части 2 ст. 50 Конституции Российской Федерации прямо обозначено, что «при осуществлении правосудия не допускается использование доказательств, полученных с нарушением федерального закона». В УПК РФ, в свою очередь, говорится о том, что доказательства, полученные с нарушением порядка, установленного уголовно-процессуальным законом, являются недопустимыми (ст. 75 УК РФ). Они не имеют юридической силы и не могут быть положены в основу обвинения, а также использоваться для доказывания любого из обстоятельств, предусмотренных ст. 73 УПК РФ.

Надо полагать, что в Конституции Российской Федерации имеется в виду обязательность соблюдения при формировании доказательств любого федерального закона, а не только уголовно-процессуального. Так, например, если сведение, которое приобрело процессуальную форму источника доказательства, получено с нарушением законодательства об оперативно-розыскной деятельности, в ходе которой и было получено, то, даже невзирая на строгое соблюдение требований УПК РФ, доказательством такое сведение считать нельзя. Оно недопустимо в качестве доказательства.

В то же время вряд ли верно полагать, что любое, даже незначительное нарушение в цепочке собирания доказательств может привести к признанию их недопустимыми[1].

По этому вопросу Н. М. Кипнис полагает, что доказательства необходимо признавать недопустимыми, только когда допущенные при их получении нарушения уголовно-процессуального закона являются существенными, иными словами, могут повлечь отмену приговора либо могут повлиять на его законность и обоснованность[2].

Конечно, процессуальная форма и формализм – понятия принципиально различные.

Формализм – соблюдение формы ради нее самой, придание ей значение самоцели, забвение содержания. Формализм в уголовном судо-

---

[1] *Миронов В.* Правила оценки допустимости доказательств // Законность. 2006. № 5. С. 35.

[2] *Кипнис Н. М.* Допустимость доказательств в уголовном судопроизводстве. Москва, 1995.

производстве – явление крайне вредное. Процессуальная форма должна соблюдаться, поскольку является гарантией обеспечения прав личности, позволяет достичь правильного результата в ходе производства.

Пленум Верховного Суда Российской Федерации подчеркивает, что доказательства должны признаваться полученными с нарушением закона, если при их собирании и закреплении были нарушены гарантированные Конституцией Российской Федерации права человека и гражданина, или установленный уголовно-процессуальным законодательством порядок их собирания и закрепления, а также если собирание и закрепление доказательств осуществлено ненадлежащим лицом или органом, либо в результате действий, не предусмотренных процессуальными нормами[1].

Вряд ли есть основания полагать, что недопустимость сведений в качестве доказательств влечет любое нарушение закона. Отдельные нарушения могут не повлиять на содержание процессуальных гарантий правосудия или защиты прав и законных интересов личности. Ответственность за такие нарушения, несомненно, также должна наступать, однако не всегда в виде санкций ничтожности доказательства.

Следует дифференцировать процессуальные санкции также в отношении обвинительных и оправдательных доказательств в зависимости от того, какая именно гарантия пострадала в результате допущенного нарушения (правило об асимметрии доказывания). В самом деле, если в ходе процессуального действия нарушена гарантия прав обвиняемого (подозреваемого), и при этом получено оправдательное доказательство, признание такого доказательства недопустимым лишь усугубит его положение[2].

Таким образом, можно выделить следующие условия допустимости доказательств:

1) субъект собрания доказательств должен иметь полномочия на проведение процессуального действия по собиранию доказательств;

2) источник сведений о фактах (источник доказательства) должен быть указан в законе;

3) способ собирания, закрепления и проверки сведений о фактах должен быть предусмотрен законом;

---

[1] О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия: постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 г. № 8 // Бюллетень Верховного Суда Российской Федерации. 1996. № 2.

[2] Подробнее об этом см.: *Победкин А. В., Гавриков В. А.* О некоторых проблемах определения допустимости доказательств в уголовном процессе // Государство и право. 1999. № 7. С. 53–56.

4) порядок собирания, закрепления и проверки сведений о фактах должен соответствовать закону (с учетом требования об асимметрии доказывания и существенности нарушения).

Недопустимые в качестве доказательств сведения не могут быть использованы в уголовно-процессуальном доказывании вне зависимости от степени их достоверности. Собственно, в случае нарушения закона при получении доказательства его достоверность всегда может быть поставлена под сомнение, поскольку именно соблюдение процессуальной формы выступает основой процессуальной гарантией соответствия сведения реальным обстоятельствам.

По этой причине нельзя согласиться с подходом к достоверности как основному предмету проверки доказательств. Именно так считают некоторые авторы[1].

Достоверность доказательства иногда рассматривают как его свойство[2], равно как свойством иногда называют и достаточность[3]. Достоверность, действительно, устанавливается в процессе доказывания, далеко не всегда она очевидна сразу[4]. Однако установление недостоверности сведения о факте не означает, что доказательство отсутствует, оно есть, хотя основывать на нем процессуальные решения ни в коем случае нельзя. Сведение о факте, обладающее относимостью и допустимостью, представляет собой доказательство вне зависимости от того, достоверно оно или нет. С точки зрения достоверности оценивается уже существующее доказательство. Будь достоверность свойством доказательства, в случае признания доказательств, собранных следователем недостоверными уже в суде, надо было бы сделать ошибочный вывод, что следователь составлял обвинительное заключение вообще не имея никаких доказательств[5], что, конечно, абсурдно. В этой связи достоверность представляет собой требование, предъявляемое к доказательствам, позволяющее использовать его для обоснования процессуальных решений.

---

[1] *Громов Н. А., Зайцева С. А., Гущин А. Н.* Доказательства: их виды и доказывание в уголовном процессе. Москва, 2006. С. 71.

[2] *Алексеев Н. С., Даев В. Г., Кокорев Л. Д.* Очерк развития науки советского уголовного процесса. Воронеж, 1980. С. 23; *Костенко Р. В.* Указ. соч. С. 63–64; *Орлов Ю. К.* Основы теории доказательств в уголовном процессе: научно-практическое пособие. Москва: Проспект, 2000. С. 54; *Будников В.* Юридическая сила доказательств в уголовном судопроизводстве // Рос. юстиция. 2003. № 10. С. 45–46.

[3] *Костенко Р. В.* Указ. раб. 2006; *Орлов Ю. К.* Основы теории доказательств в уголовном процессе: научно-практическое пособие. Москва: Проспект, 2000. С. 63.

[4] Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. 2-е изд., испр., и доп. Москва: Юрид. лит., 1973. С. 222.

[5] *Кокорев Л. Д., Кузнецов Н. П.* Указ. соч. С. 135.

Согласно ст. 88 УПК РФ каждое доказательство подлежит оценке с точки зрения относимости, допустимости, достоверности, а все собранные доказательства в совокупности – достаточности для разрешения уголовного дела. Невзирая на формулировку ст. 88 УПК РФ, совокупность доказательств подлежит оценке с точки зрения достаточности для принятия любых уголовно-процессуальных решений в ходе судопроизводства. Достаточность доказательств – требование, предъявляемое не к отдельно взятому доказательству, а к их совокупности. Именно поэтому достаточность никак не может считаться свойством доказательства. Недостаточность для принятия решения уголовно-процессуальных доказательств не означает, что каждое сведение доказательством не является. Возможно, в ходе дальнейшего производства будут получены доказательства, позволяющие сформировать их достаточную совокупность.

В литературе предлагают выделять и иные свойства доказательств, например, конвергентность[1], сила (значимость)[2]. Однако в целом такие мнения широкой поддержки не получили. Они имеют слабые места, на которые авторы настоящей работы ранее указывали[3].

Спроецировав изучение общетеоретических положений о свойствах доказательств на тему исследования и содержание настоящего параграфа, обратим внимание, что проверка и оценка доказательственной информации, содержащихся на электронных носителях, осуществляются сквозь призму указанных характеристик сведений, имеющих значение для расследования уголовных дел. При этом и проверка, и оценка доказательственной информации, содержащейся на электронных носителях, имеют особенности, находящиеся, конечно, в рамках общих процессуальных правил.

Применительно к особенностям доказательственной информации, содержащейся на электронных носителях, имеются сложности, которые возникают при ее проверке. Так, на электронных носителях зачастую содержится огромное количество файлов, а необходимая для использования в процессе доказывания информация может быть скрыта или уничтожена, вследствие чего для обнаружения или восстановления такой информации требуется специальное программное аппаратное обеспечение, а также специальные знания.

---

[1] *Будников В.* Юридическая сила доказательств в уголовном судопроизводстве // Рос. юстиция. 2003. № 10. С. 45–46.

[2] *Орлов Ю. К.* Основы теории доказательств в уголовном процессе: научно-практическое пособие. Москва: Проспект, 2000. С. 57.

[3] *Победкин А. В.* Уголовно-процессуальное доказывание. Москва: Юрлитинформ, 2009. С. 165–172; и др.

В этой связи справедливо мнение В. Н. Григорьева и О. А. Максимова, которые считают, что специфика формирования цифровой информации, вне зависимости от производства по делу, действительно требует дополнительных гарантий ее достоверности[1].

По мнению П. С. Пастухова, допустимость информации устанавливается с учетом соответствия реквизитов компьютерной информации, таких как тип файла, его объем, время создания, время редактирования, время открытия, сведения о пользователе; установления, каким образом было обеспечено условие ее целостности, а также с учетом соответствия типа (вида) программного средства, которое использовалось для:

1) формирования (создания) данной информации;

2) ее копирования, если данная информация была перенесена на другой носитель;

3) воспроизведения данной информации (характеристики программных средств, например типа операционной системы, регистрационного номера лицензии и пр.)[2].

Очевидно, современные технологии открывают значительный простор для всевозможных манипуляций с такой информацией, что может создавать предпосылки для признания ее недопустимым доказательством[3]. В этих условиях необходимо развивать процессуальные гарантии при собирании доказательств, имеющих в своей информационной основе сведения, содержащиеся на электронных носителях.

При этом выше уже было отмечено, что обязательное участие специалиста при изъятии электронных носителей информации нарушает принцип процессуальной экономии, поскольку его роль сводится к упаковке предметов, производство которой может быть осуществлено следователем.

Согласно информации, полученной из следственных органов различных регионов России, на практике считают, что участие специалиста целесообразно при необходимости отсоединения электронного устройства от сети либо демонтажа устройства для изъятия его составных частей.

---

[1] *Григорьев В. Н., Максимов О. А.* Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. № 2 (84). С. 34.

[2] *Пастухов П. С.* Средства проверки надежности «электронных» доказательств в ходе производства по уголовному делу // Пробелы в российском законодательстве. 2015. № 3. С. 170.

[3] *Гаврилин Ю. В., Победкин А. В.* Модернизация уголовно-процессуальной формы в условиях информационного общества // Труды Академии управления МВД России. 2019. № 3 (51). С. 28.

Факт копирования информации на иной носитель по ходатайству владельца данной информации и с целью передачи этого носителя последнему является обеспечением прав и законных интересов физических и юридических лиц, но не гарантией достоверности получаемой информации. Напротив, присутствие специалиста при копировании информации для приобщения электронного носителя, на который она была скопирована, к уголовному делу, служит достоверности формируемого доказательства. Однако именно в данном случае законодатель и не предусмотрел обязательного участия специалиста.

Анализ изученных уголовных дел показал, что основанием для обжалования результатов следственных действий в 92 % случаев являлось нарушение прав их участников. Результаты опроса практических работников выглядят следующим образом: на вопрос, обжаловались ли участниками уголовного судопроизводства результаты следственных действий в связи с нарушением их прав при изъятии электронного носителя информации, отрицательно ответили 68,8 % респондентов, 32,2 % констатировали обжалование результатов следственных действий, при этом 14,3 % указали причину в несоответствии квалификации специалиста, 2,9 % отметили, что не предоставлена возможность копирования информации, 31 % указали на причину производства изъятия электронного носителя информации без специалиста.

Анализ изученных приговоров, в которых имеются цифровые доказательства, показал, что в 80 % случаев данные доказательства остаются в уголовном деле без изменения, но бывают случаи, когда цифровые доказательства признаются недопустимыми.

Например, постановлением Майкопского городского суда было удовлетворено ходатайство защитника о признании не допустимыми доказательствами мобильных телефонов «Samsung» и «Philips» и их содержимого. Указанным постановлением признаны недопустимыми доказательствами и исключены из их числа: мобильный телефон «Samsung», мобильный телефон «Philips» и содержимое телефонов, протокол осмотра предметов (телефонов), заключение компьютерно-технической экспертизы.

Суд разъяснил, что в соответствии с пп. «а» п. 5 ч. 2 ст. 82 УПК РФ вещественные доказательства в виде электронных носителей информации хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации. Между тем, при исследовании доказательств в ходе судебного разбирательства было установлено, что

с изъятых телефонов производились звонки и отправлялись SMS-сообщения после их изъятия и упаковки[1].

Следующей особенностью проверки электронных доказательств является необходимость обращения к помощи специалиста в ходе работы с такими доказательствами. Более подробно данная проблема исследовалась нами в первом параграфе данной главы.

Проверка источника доказательственной информации на электронных носителях предполагает, что должны сохраняться подлинники электронных носителей, которые помогут установить отсутствие внесений модификаций с помощью технических средств. Изучение нами уголовных дел показало, что в 15 % случаев лица, у которых непосредственно изымались электронные носители информации, пытались уничтожить информацию, содержащуюся на них. Результаты опроса практических работников подтвердили наше предположение о том, что попытки уничтожения информации и (или) ее носителей после изъятия информации путем копирования в порядке, предусмотренном ст. 164.1 УПК РФ, не предпринимались (89,3 %), столкнулись же с этой проблемой 10,6 % опрошенных.

Требует внимания факт установления подлинности источника доказательства на электронном носителе и отсутствия модификации находящейся на нем информации. Необходимо установление источника происхождения информации на электронном носителе, идентификация ее автора и аутентификация ее владельца (пользователя), что будет являться необходимыми условиями проверки такого свойства доказательства, как его достоверность.

Аутентичность – это свойство электронного документа, которое позволяет доказать авторство документа, время создания и подлинность его содержания.

Федеральный закон «Об электронной цифровой подписи»[2] определяет, что электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Средством проверки документа в электронном виде будет наличие электрон-

[1] Приговор Майкопского городского суда от 12.04.2016 № 1-351/2015 1-5/2016 по делу № 1-351/2015.

[2] Об электронной цифровой подписи: федеральный закон от 10 января 2002 г. № 1-ФЗ // Собр. законодательства Рос. Федерации. 2002. № 2. Ст. 127.

ной цифровой подписи, в связи с чем документ приобретает юридический статус и имеет такую же юридическую силу, как бумажный документ с собственноручной подписью и печатью.

Наличие цифровой подписи поможет проконтролировать целостность документа. Если по какой-то причине документ будет изменен, то подпись станет недействительной, так как она подтверждает только первоначально созданный документ, кроме того, электронная подпись – защита от подделки документа.

По этому вопросу Т. С. Астахова и Е. П. Чадаева[1] справедливо отмечают: чтобы создать корректную подпись, необходимо знать закрытый ключ, а он должен быть известен только владельцу, поэтому владелец документа не может отказаться от своей подписи и, соответственно, отказ от авторства невозможен.

Под идентификацией понимается возможность установления лица, от которого получен электронный документ[2]. В необходимых случаях должны быть представлены экспертные заключения, подтверждающие отсутствие внесения изменений в электронные документы. В некоторых работах предлагается осуществлять пошаговое документирование идентификационных свойств файла при каких-либо действиях с ним, в частности при перемещении[3].

При изготовлении протокола следственного действия необходимо указывать ряд признаков, которые определяют аутентичность информации, скопированной специалистом (количество скопированных файлов, их размер как в отдельности, так и в совокупности, наименование файлов и т. д.). Полагаем, что это будет являться правовой гарантией во избежание дальнейшего искажения либо модификации изъятой информации.

Уместно будет упомянуть о Международной организации по компьютерным доказательствам, которая на сегодняшний день является признанным лидером в области исследования и оценки доказательственного значения компьютерной информации и цифровых доказательств. Целью работы данной организации является предоставление правоохранительным органам всех стран научной и методической информации по вопросам судебно-экспертного исследования компьютеров, компьютерных программ и баз данных.

---

[1] *Астахова Т. С., Чадаева Е. П.* Электронная цифровая подпись как фактор сохранения целостности и аутентичности документа // Известия Томского политехнического университета. 2012. № 6. С. 153.

[2] *Зайцев П.* Электронный документ как источник доказательств // Законность. 2002. № 4. С. 43–44.

[3] *Александров А. С., Кувычков С. И.* О надежности «электронных доказательств» в уголовном процессе // Библиотека криминалиста: науч. журнал. 2013. № 5 (10). С. 82.

Данной организацией были сформулированы принципы работы при проверке компьютерной информации:

– во время работы с цифровыми доказательствами должны соблюдаться все общие судебно-экспертные процедурные принципы;

– действия по исследованию изъятых цифровых доказательств не должны вносить в них изменений;

– в случае необходимости предоставления кому-либо доступа к оригиналу цифрового доказательства он должен быть обучен и проинструктирован соответствующим образом;

– вся деятельность, касающаяся конфискации (изъятия), доступа, хранения и передачи цифрового доказательства, должна быть полностью документирована и доступна для ознакомления;

– лицо, в распоряжении которого находится цифровое доказательство, полностью ответственно за все действия, предпринятые относительно этого доказательства;

– любое агентство, которое является ответственным за выборку из памяти, изъятие, хранение или передачу цифрового доказательства, ответственно за согласие с этими принципами[1].

Существует мнение, что не всегда возможно установить аутентичность цифровых доказательств. Например, Е. И. Галяшина[2], считает, что сложность в процессуальной проверке и оценке достоверности цифровых фонограмм, даже подтвержденных с помощью технологии цифровой подписи, заключается в принципиальной возможности их мистификации без оставления каких-либо следов проведенных манипуляций, в отсутствии в настоящий момент криминалистических методик и эффективных экспертных рекомендаций установления аутентичности цифровых фонодокументов, что затрудняет их допустимость в качестве основы формирования доказательств в уголовном судопроизводстве.

Затрагивая данный вопрос в своей работе, Н. А. Зигура[3] говорит о том, что по отношению к компьютерной информации на этапе проверки должны соблюдаться определенные правила, к которым она относит: установление технического средства, с какого была получена или скопирована данная информация; проверку соответствия типа, модели, фирмы изготовителя материального носителя компьютерной информации с параметрами, указанными в протоколе следственного

[1] *Хазиев Ш. Н.* Международное сотрудничество в области судебной компьютерно-технической экспертизы // Библиотека криминалиста: науч. журнал. 2013. № 5. С. 302.

[2] *Галяшина Е. И.* Теоретические и прикладные основы судебной фоноскопической экспертизы: автореф. дис. ... д-ра юрид. наук. Воронеж, 2002.

[3] *Зигура Н. А.* Компьютерная информация как вид доказательств в уголовном процессе России: дис ... канд. юрид. наук. Челябинск, 2010. С. 144.

действия, в заключении специалиста; установление программного средства, с помощью которого была получена данная информация.

Изъятие следователем доказательственной информации с электронных носителей в строгом соответствии с процессуальными нормами и разработанными методиками является важнейшей гарантией допустимости доказательств, получаемых в ходе осмотров электронных носителей информации, сопровождаемых выемкой, а также в ходе обысков и выемок электронных носителей информации.

Так, например, обвиняемый П. обратился в суд с жалобой в порядке ст. 125 УПК РФ, в которой просил признать незаконным и необоснованным отказ следователя в удовлетворении заявленного ходатайства о предоставлении для ознакомления с возможностью копирования своими техническими средствами приложений к экспертным заключениям, подготовленным в электронном виде по уголовному делу, а также содержимого указанных в ходатайстве вещественных доказательств в виде электронных носителей информации, иных вещественных доказательств и фотографий, материалов аудио- и (или) видеозаписи, киносъемки и иных приложений к протоколам следственных действий), полагая, что доводы следователя, послужившие основанием для отказа в удовлетворении данного ходатайства, не основаны на законе.

Судами первой и апелляционной инстанций обвиняемому отказано в удовлетворении жалобы на основании того, что любое подключение накопителей информации после проведения компьютерно-технических судебных экспертиз без использования специализированного криминалистического программно-аппаратного комплекса может повлечь нарушение целостности содержимого накопителей информации.

С точки зрения относимости оценивается как содержание компьютерной информации, так и ее свойства: дата создания, изменения, открытия. При этом установление связи электронного доказательства с обстоятельствами, имеющими значение для уголовного дела, часто требует участия специалиста или же проведения экспертизы. Кроме того, доказательственная информация, полученная с электронных носителей, будет обладать признаком относимости, если будет обоснована логическая связь полученных сведений с теми, что необходимо установить по конкретному уголовному делу с целью правильного его разрешения.

Проведение судебной экспертизы электронных носителей информации, в результате которой в уголовном деле появится доказательственная информация, полученная с данных носителей, также требует внимания при возникновении вопроса достоверности полученной информации. Прежде всего само постановление о назначении судебной экспертизы должно соответствовать требованиям,

изложенным в законе, которые обеспечивают допустимость и достоверность сведений. Это значит, что, помимо правильной постановки вопросов эксперту, предоставления ему в упакованном и опечатанном виде электронного носителя информации, с постановлением о ее назначении должны быть ознакомлены участники уголовного судопроизводства, обладающие правом на такое ознакомление.

При оценке экспертного заключения необходимо удостовериться, что эксперт не вышел за пределы своей компетенции и им были соблюдены все правила проведения экспертизы. В связи с тем, что первичная информация, находящаяся на электронном носителе, может быть легко изменена или уничтожена, в том числе и экспертом, последним необходимо руководствоваться принципами работы с информацией на электронных носителях, которые были разработаны Международной организацией по компьютерным доказательствам, о которой упоминалось ранее.

По мнению П. С. Пастухова, компьютерно-техническая экспертиза является специальным средством проверки электронных доказательств. При этом сомнения в достоверности доказательственной информации, полученной с электронных носителей, могут быть вызваны тем, что в такую информацию легко внести изменения, которые без помощи эксперта будет сложно обнаружить.

При определении достаточности как свойства доказательств применительно к цифровой информации собирать всю имеющуюся на исследуемом электронном носителе информацию необходимости нет. При этом надо отметить, что проверка и оценка электронных доказательств, с одной стороны, естественно подчиняются общим закономерностям, присущим проверке и оценке доказательств по уголовным делам. С другой стороны, вследствие специфики объектов цифровой информации проверка и оценка электронных доказательств требуют применения специальных знаний о природе такого рода информации, а также использования в необходимых случаях соответствующего программного-аппаратного обеспечения.

При оценке доказательственной информации на электронных носителях должно учитываться следующее:

1) надежность способа, с помощью которого подготавливалась, хранилась или передавалась электронная информация;

2) надежность способа, при помощи которого обеспечивалась целостность информации;

3) надежность способа, при помощи которого идентифицировался его составитель;

4) правильность способа фиксации информации, в связи с тем, что закрепление информации на современном источнике может отражаться на достоверности данного доказательства[1].

В любом случае следователь должен обладать соответствующими знаниями в области информатики хотя бы начального уровня, поскольку неосторожный доступ к такого рода информации может привести к потери доказательственного значения интересующей информации.

Закрепление или фиксация собранной доказательственной информации на электронных носителях подразумевает перенос данной информации на иной, процессуальный источник информации. При этом необходимо удостовериться в том, что искомая информация находится на первичном источнике.

Признавая, несомненно, высокое значение для определения допустимости информации на электронном носителе изложенных выше факторов, полагаем, что в основу перечня критериев допустимости информации на электронных носителях должны быть положены требования, предусмотренные ГОСТ Р ИСО 15489-1-2019 «Информация и документация. Управление документами»[2]. С учетом сказанного полагаем, что система специфических критериев оценки допустимости доказательственной информации на электронных носителях включает в себя:

1. Аутентичность информации как возможность достоверного установления источника ее происхождения, создавшего ее лица или процесса, порядка (процедур) ее создания. При решении вопроса об аутентичности доказательственной информации, находящейся на электронном носителе, принципиально важным является проверяемость источника ее происхождения, которая, в свою очередь, обеспечивается максимальной детализацией при описании порядка ее обнаружения и изъятия в протоколе следственного действия. С указанной целью в протоколе следственного осмотра (обыска, выемки) подлежит отражению место расположения изъятой информации в обследуемой информационной системе с указанием сетевого адреса (в случае изъятия информации с сетевых носителей) либо соответствующего каталога (папки). Если поиск информации осуществлялся с использованием специального программно-аппарат-

[1] *Нахова Е. А.* Проблемы электронных доказательств в цивилистическом процессе // Ленинградский юридический журнал. 2015. № 4. С. 302.

[2] ГОСТ Р ИСО 15489-1-2019. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Ч. 1. Понятия и принципы: утв. приказом Росстандарта от 26.03.2019 № 101-ст, введен в действие с 1 января 2020 г.

ного обеспечения (например «Мобильный криминалист», PC-3000 и др.), то в протоколе подлежат отражению результаты его применения: формализованные отчеты программы, фотоснимки экрана с результатами ее работы, так называемые «скриншоты» – созданные с использованием стандартных средств операционной системы изображения, показывающие в точности то, что видит пользователь на экране[1]. Кроме того, в протоколе должны быть отражены метаданные изымаемых (скопированных) файлов и (или) размерные характеристики (форм-фактор) электронного накопителя в случае, если он изымается вместе с хранящейся информацией.

Исключительно важное процессуальное значение имеет упаковка изымаемого электронного носителя информации, материал которой должен исключать возможность дистанционного считывания находящейся на нем информации.

2. Достоверность информации – точное отражение определенных явлений, процессов, деятельности или фактов. Данная характеристика определяется механизмом (технологией) создания информации, например, при использовании видеорегистратора, получении записи камеры наружного видеонаблюдения, электронного журнала протоколирования событий в информационной системе, отправки электронной почты, размещения сообщения в социальной сети и т. д. Важнейшим критерием достоверности информации, находящейся на электронном носителе, является соответствие метаданных файла обстоятельствам его создания. Метаданные файла представляют собой техническую сопутствующую информацию о признаках этого файла: дату и время создания, автора, размер, тип используемого программного обеспечения и его версию и другие признаки, в зависимости от типа данных. Так, метаданные фотоизображений могут содержать сведения о марке и модели фотокамеры, метки геолокации, позволяющие определить место съемки и иные параметры[2].

Достоверность информации проявляется и в научности методов восстановления уничтоженных и поврежденных данных, а также данных, доступ к которым ограничен с применением средств криптографической защиты. Как справедливо указывает Н. А. Зигура,

[1] Более подробно см.: *Гаврилин Ю. В.* Криминалистические особенности обнаружения, фиксации, изъятия и исследования электронных следов преступления // Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: в 2 ч. / А. В. Аносов [и др.]. Москва: Академия управления МВД России, 2019. Ч. 1. С. 105–131.

[2] Более подробно см.: *Балашова А. А.* Оценка допустимости доказательств в виде информации на электронных носителях // Евразийский юридический журнал. 2020. № 2. С. 334–335.

используемое в указанных целях программное обеспечение должно быть сертифицировано[1] *в соответствии с требованиями действующего законодательства* (курсив – авт.).

3. Целостность информации как отсутствие изменений в ее составе, содержании и свойствах. Средствами обеспечения целостности информации на электронном носителе, полученной в процессе производства следственного действия, могут являться:

1) использование для изъятия информации посредством ее копирования электронных носителей, не допускающих перезаписи (в частности CD-R-дисков)[2];

2) архивирование изымаемой информации без возможности ее изменения[3], использование при этом криптографической хэш-функции, позволяющей на основе математических алгоритмов осуществлять преобразование произвольного массива данных в состоящую из букв и цифр строку фиксированной длины[4]. Одним из распространенных алгоритмов хеширования является MD5, который преобразовывает исходную информацию произвольного размера в хэш – псевдослучайную последовательность символов фиксированной длины, представляющий собой своего рода «отпечаток информации» – идентификатор зашифрованного массива данных[5];

3) использование электронной подписи должностного лица, проводящего следственное действие, для удостоверения целостности информации. В соответствии со ст. 2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» она представляет собой информацию в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В соответствии со ст. 6 указанного закона информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному

---

[1] *Зигура Н. А.* Компьютерная информация как вид доказательств в уголовном процессе России: дис. ... канд. юрид. наук. Челябинск, 2010. С. 145.

[2] *Григорьев В. Н., Савенков А. В.* О цифровых технологиях фиксации сведений по уголовному делу // Уголовная юстиция. 2018. № 12. С. 67.

[3] *Газизов В. А.* Особенности исследования цифровых видеопортретов // Вестник Московского университета МВД России. 2017. № 2. С. 123.

[4] Энциклопедия «Касперского». Хэширование: сайт. URL: https://encyclopedia.kaspersky.ru/glossary/hashing/ (дата обращения: 15.03.2020).

[5] Энциклопедия «Касперского». MD5: сайт. URL: https://encyclopedia.kaspersky.ru/glossary/md5/ (дата обращения: 15.03.2020).

собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

4. Доступность для восприятия с использованием надлежащего программного обеспечения и технических средств обработки, не влекущих внесение в нее изменений. Особенностью цифровой информации является невозможность ее непосредственного (зрительного, тактильного, слухового и пр.) восприятия человеком. Для этой цели применяется специальное программное обеспечение, преобразующее информацию в доступный для восприятия человеком вид. При этом принципиально важно, чтобы подобное преобразование информации, осуществляемое в процессе ее воспроизведения, не модифицировало ни саму информацию, ни присущие ей метаданные. Иное означало бы уничтожение аутентичной информации и ее подмену некой производной информацией, допустимость которой будет вызывать значительные сомнения.

Авторами настоящего пособия ранее по этому поводу отмечалось, что если в ходе следственного действенного действия производится копирование информации с электронных носителей без изъятия последних, то в этом случае в протоколе следственного действия или приложении к нему подлежат отражению признаки, свидетельствующие об аутентичности скопированной информации[1]. Законодательное требование указания таких признаков будет являться дополнительной правовой гарантией, исключающей возможность впоследствии какой-либо модификации скопированной информации. К таким признакам можно отнести: общее количество скопированных файлов, количество файлов того или иного типа, их общий размер, а также контрольную сумму – числовое значение, рассчитанное по особому алгоритму и программным обеспечением, используемым для копирования информации, и предназначенное для проверки целостности и неизменности скопированной информации.

В заключение параграфа приходим к выводу о необходимости использования специфических критериев оценки допустимости доказательственной информации на электронных носителях, к числу которых относятся:

---

[1] *Гаврилин Ю. В., Победкин А. В.* Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствовать процессуальные формы // Труды Академии управления МВД России. 2018. № 3 (47). С. 109.

– аутентичность информации как возможность достоверного установления источника ее происхождения;

– целостность информации как отсутствие изменений в ее составе, содержании и свойствах;

– достоверность информации – точное отражение определенных явлений, процессов, деятельности или фактов;

– доступность для восприятия с использованием надлежащего программного обеспечения и технических средств обработки, не влекущих внесение в нее изменений.

Вопросы для повторения

1. Понятие и содержание проверки и оценки доказательств.
2. Правила оценки доказательств.
3. Понятие и содержание аутентичности информации.
4. Понятие и содержание целостности информации.
5. Понятие и содержание достоверности информации и доступности ее для восприятия.

Практическое задание

Защитником заявлено ходатайство о признании недопустимым доказательства – заключения эксперта, установившего содержание переписки подозреваемого с использованием сервиса электронной почты, на том основании, что исследуемый экспертом файл – и файл, содержащийся в компьютере подозреваемого, отличаются между собой своими метаданными. Каковы процессуальный и тактические средства разрешения сложившейся ситуации?

§ 3. Основные направления использования криминалистически значимой информации, полученной при исследовании электронных носителей, в процессе расследования преступлений

Современные информационно-телекоммуникационные технологии, основанные на использовании ресурсов сети Интернет, позволяют подготавливать, совершать и скрывать преступления дистанционным способом, исключающим непосредственный контакт соучастников как между собой, так и с третьими лицами. Дистанционный способ совершения преступлений предполагает, что все взаимные коммуникации причастных к ним лиц осуществляются опосредованно, с использованием технологических возможностей интернет-сервисов: социальных сетей, электронной почты, сервисов мгновенных сообщений (например ICQ, WhatsApp, Viber, Skype, Telegram), сайтов неиндексируемой части Интернта (т. н. Даркнет) и т. п. Кроме того, широкие возможности для подготовки, совершения и сокрытия преступлений предоставляют электронные платежные системы и цифровая валюта.

Проведенные исследования позволяют констатировать, что знание закономерностей образования криминалистически значимой информации в цифровой форме (следовой картины) позволяет эффективно решать тактические задачи, возникающие в процессе выявления, раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, включая установление события преступления, совершившего его лица (лиц), содержания действий при совершении преступления и т. п. В качестве доказательств электронные носители информации могут использоваться при расследовании преступлений, возбужденных практически по всем статьям особенной части Уголовного кодекса Российской Федерации, начиная с «традиционных» корыстных преступлений (кража, мошенничество и т. д.) и заканчивая «компьютерными преступлениями», предусмотренными гл. 28 УК РФ. Получение и использование доказательственной информации, содержащейся на электронных носителях, по уголовным делам является одной из основных и трудно решаемых на практике задач, требующей наличия специальных познаний в области компьютерной техники и программного обеспечения. Корректное изъятие электронных носителей информации требует наличия специальных технических устройств и привлечения к участию в их изъятии специалистов в соответствии со ст. 164.1 УПК РФ.

Положительными примерами использования доказательственной информации, полученной с помощью изъятых электронных носителей информации при расследовании преступлений, могут служить уголовные дела:

1) по обвинению М., Ш., У., У. в совершении преступлений, предусмотренных п. «а», «б» ч. 6 ст. 171 УК РФ, ч. 4 ст. 327.1 УК РФ, ч. 4 ст. 180 УК РФ, по факту производства и хранения в целях сбыта немаркированной алкогольной продукции, в ходе расследования которого был осмотрен системный блок компьютера, изъятый в ходе обыска по месту проживания М. по адресу: г. Брянск, Советский район, ул. Фокина, д. 43, кв. 6, в котором установлен накопитель на жестких магнитных дисках (НЖМД), «Seagate», модель ST500DM002, 500Gb, S/N: Z6E66ZZM. В ходе осмотра было установлено, что на данном НЖМД содержатся в файлах в электронном варианте бланки документов, которые использовались для перевозки алкогольной продукции, также фотографии алкогольной продукции, графики работы. Данные файлы были записаны на оптический диск CD-R однократной записи;

2) по обвинению З., И., Т., М. в совершении преступлений, предусмотренных ч. 4 ст. 159.2, ч. 4 ст. 159.2, ч. 4 ст. 159.2, ч. 4 ст. 159.2, ч. 4 ст. 159.2, ч. 4 ст. 159.2 УК РФ по факту мошенничеств при получении компенсации в соответствии с Законом РФ от 15.05.1991 № 1244-1 «О социальной защите граждан, подвергшихся воздействию радиации вследствие катастрофы на Чернобыльской ГАЭС» путем представления заведомо ложных и недостоверных сведений, в ходе расследования которого был осмотрен изъятый протоколом выемки в департаменте строительства Брянской области системный блок персонального компьютера, находившегося в пользовании Т. Осмотром установлено, что в памяти указанного устройства обнаружены списки граждан на получение компенсации материального ущерба в связи с утратой имущества вследствие катастрофы на Чернобыльской АЭС за период 2016 и 2017 гг., в которых отражены сведения о включенных в них гражданах, претендующих на получение выплат, среди которых указаны фамилии подставных лиц и суммы денежных средств, подлежащие выплате указанным гражданам за утрату имущества;

3) по обвинению К., Х., Б., М. в совершении преступления, предусмотренного п. «а, б» ч. 4 ст. 158 УК РФ, по факту тайного хищения дизельного топлива Евро Сорт С, принадлежащего АО «Транснефть-Дружба»» в количестве 371 тонны 157 килограммов, общей стоимостью 14 614 365 рублей 87 копеек, в особо крупном размере путем незаконной врезки в МНПП «Куйбышев-Брянск» на 1 108

километре участка ЛПДС «Стальной Конь – Брянск», в ходе расследования которого осмотрен мобильный телефон, изъятый в ходе личного обыска подозреваемого К., и находящиеся в его пользовании личные электронные записи обвиняемого – заметки о получении гражданства Канады; номера банковских карт; движение денежных средств; изъята электронная переписка, содержащаяся в почтовом ящике 89169114270 Qrambler.ru, которая перенесена на физический носитель, а именно DVD-R диск с надписью «89169114***», анализ переписки позволяет сделать вывод, что обвиняемый К. (действуя от лица «С.») как лидер организованной группы использовал данный электронный почтовый ящик для дистанционного документооборота в условиях конспирации для достижения преступных целей организованной группы и минимизации рисков обнаружения; осмотрены предметы, изъятые в ходе личного обыска подозреваемого К., в частности: записывающее устройство (диктофон) «SONY ICD-11X502» и ноутбук «HP». При осмотре диктофона «SONY ICD-UX502» установлено, что на устройстве расположен звуковой файл длительностью 10 минут 45 секунд. Файл в ходе осмотра воспроизведен, и прослушиванием установлено, что на файле зафиксирован диалог, опровергающий показания обвиняемого К. После прослушивания аудиозапись скопирована на ПК «AQUARIUS» и с помощью программы «NERO» записана на чистый CD-R диск для приобщения в качестве приложения к протоколу. Далее, в ходе осмотра ноутбука часть документов перенесена на бумажный носитель. Анализ обнаруженных *документов позволил сделать вывод следователю о* длительном существовании организованной группы под руководством К., который в целях конспирации, используя несуществующие персональные данные, осуществлял организаторские функции по типовой схеме (приискание с целью аренды помещений, земельных участков, изготовление подложных договоров, накладных и т. д.) в интересах преступной группы;

4) по обвинению П. и К. в совершении преступлений, предусмотренных ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ; ч. 3 ст. 30, п. «а», «г» ч. 4 ст. 228.1 УК РФ по факту бесконтактного сбыта наркотических средств на территории г. Брянска, в ходе расследования которого компьютерно-техническими экспертизами установлено, что в памяти мобильного телефона «Nokia GSM 2700c-2 Classic (RM-561)» с сим-картой оператора «Теле2» обнаружены файлы аудиоформата, имеющие отношение к обстоятельствам сбыта П. наркотических средств за период с 01.04.2015 до 25.08.2015, а также SMS-сообщения, в которых содержится переписка, конкретизирующая местонахождение «закладок» наркотических средств для

потребителей; в ноутбуке «Samsung R540-JS05» имеется программное обеспечение, предназначенное для подключения и работы в глобальной сети Интернет, а также имеются признаки работы в сети Интернет и на сайте «legalrc biz»; в программе персональной связи через Интернет «Skype» обнаружены учетные записи «brik3***», «natalla32***», сообщения которых имеют отношение к обстоятельствам сбыта наркотических средств за период с 01.04.2015 до 25.08.2015; в архиве переговоров базы данных ISQ-программы передачи текстовых сообщений через Интернет обнаружены почтовые сообщения абонента +79003577*** и +79208531***, которые имеют отношение к обстоятельствам сбыта наркотических средств за период с 01.04.2015 до 25.08.2015[1].

5) по обвинению С., Г. и М., которые в период с 2012 по 2013 гг., действуя от имени инвестиционной компании «Axiomlab Company Ltd», посредством созданного ими интернет-сайта www.invest-biznes.com путем обмана похитили денежные средства более 160 граждан РФ на общую сумму более 90 млн рублей.

Так, в ходе производства обыска в жилище обвиняемого С. обнаружен и изъят смартфон. В ходе его осмотра с участием специалиста удалось восстановить удаленные SMS-сообщения, среди которых следователем обнаружено сообщение, содержащее данные физического лица и номер банковского счета, на который потерпевшие осуществляли перечисление денежных средств в качестве вкладов в инвестиционную деятельность компании.

В результате следствием установлены данные абонента Г., от которого поступило указанное сообщение обвиняемому С. В ходе обыска в жилище Грачева обнаружен и изъят накопитель на жестких магнитных дисках, содержащий информацию о создании и администрировании Г. сайта www.invest-biznes.com. Также на данном диске обнаружена переписка через интернет-службу мгновенных сообщений ICQ, содержание которой указывает на участие Г. и его собеседника в разработке и совершенствовании функциональности указанного сайта. Найдена установленная программа-клиент электронной почты «The Bat!». В составе данных указанной программы найден архив электронной почты, содержащий переписку обвиняемого С. с Г. Основная тематика обнаруженной переписки – создание, размещение в сети Интернет, информационно-функциональное наполнение и рекламное продвижение сайта www.invest-biznes.com. Кроме того, на диске содержались текстовые файлы о деятельности компании «Axiomlab Company Ltd», которые публиковались на интер-

[1] Письмо СУ УМВД России по Брянской области от 22.07.2019 № 17/8587.

нет-сайте и содержали заведомо ложную информацию о возможности получения дохода от вложения денежных средств под высокий процент с целью последующего хищения полученных от граждан денежных средств.

Кроме того, обвиняемые С. и М. привлекли более 50 физических лиц, которые за денежное вознаграждение открывали в банках г. Красноярска счета, на которые введенные в заблуждение граждане осуществляли перечисление денежных средств в качестве вкладов в деятельность «Axiomlab Company Ltd», полагая, что владельцами указанных счетов являются профессиональные трейдеры компании. В дальнейшем обвиняемый С. удаленным доступом посредством программы «Теле-банк» осуществлял управление указанными счетами, перечислял часть денежных средств на другие банковские счета привлеченных им физических лиц с целью последующего обналичивания и хищения денежных средств. При этом с целью привлечения большего количества граждан и последующего хищения денежных средств, а также создания видимости реального осуществления компанией инвестиционной деятельности частично осуществлял возврат денежных средств в размере вкладов и процентов по ним.

В ходе следствия, в результате изучения и анализа детализаций телефонных переговоров обвиняемого, установлено, что С. неоднократно обращался в службу поддержки банков. На запросы следователя банками предоставлена информация о том, что телефонные разговоры сотрудников банка с клиентами хранятся на протяжении нескольких лет. В результате в банках следователем истребованы CD-диски с записями таких разговоров. По результатам проведенных фоноскопических судебных экспертиз установлено, что голос мужчины – клиента банка, который неоднократно обращался с вопросами перевода денежных средств, представляясь фамилиями привлеченных им физических лиц, принадлежит обвиняемому С.

Таким образом, обнаруженные и изъятые в ходе производства обысков электронные носители информации, сотовый телефон, накопитель на жестких магнитных дисках, а также предоставленные банком по запросу следователя CD-диски использовались в качестве доказательств причастности С. и Г. к совершению мошенничества в отношении более 160 граждан РФ в особо крупном размере.

Уголовное дело направлено в суд, постановлен обвинительный приговор[1];

[1] Письмо ГСУ ГУ МВД России по Красноярскому краю от 25.07.2019 № 4/9492.

6) по обвинению К. в совершении преступлений, предусмотренных ч. 2 ст. 273 и ч. 4 ст. 159.6 УК РФ, по фактам хищений денежных средств со счетов банковских карт клиентов ПАО Сбербанк посредством использования вредоносной компьютерной программы, выделенное 18.04.2018 в отдельное производство в порядке ч. 2 ст. 154 УПК РФ из уголовного дела № 62359, находившегося в производстве СЧ ГСУ ГУ МВД России по Московской области.

По указанному уголовному делу в жилищах обвиняемого К. и иных участников организованной группы изъяты мобильные телефоны, флеш-накопители, ноутбуки, которые осмотрены и признаны вещественными доказательствами. В ходе осмотра ноутбуков, проведенных с участием специалистов, на одном из них обнаружена база данных всех зараженных мобильных устройств, а содержимое интернет-ресурсов, которые администрировались с изъятых ноутбуков, записано на DVD-R диски, впоследствии предоставленные сотрудникам ЭКЦ для проведения компьютерной экспертизы, по результатам которой установлено, что определенные вебсайты являются панелями управления программным обеспечением, установленным на мобильных устройствах, к функциональным возможностям которых относятся: регистрация мобильных устройств с установленным программным обеспечением, получение и обработка информации о мобильных устройствах, выдача установленному на мобильных устройствах программному обеспечению команд на перехват входящих и исходящих SMS-сообщений, а также их отправку SMS-сообщений на заданные номера, отправку USSD-команд и сбор статистики.

Также в ходе следствия изымались мобильные телефоны и смартфоны, принадлежащие потерпевшим, явившиеся объектами компьютерных судебных экспертиз, по результатам которых установлено наличие на них программ, в функции которых входят скрытые от пользователя отправка и чтение коротких текстовых сообщений SMS, отправка запросов USSD, сокрытие или удаление коротких текстовых сообщений, обращение к ресурсам в сети Интернет для получения и передачи какой-либо информации[1];

7) по обвинению Г. в совершении преступления, предусмотренного ч. 4 ст. 159 УК РФ.

Предварительным следствием установлено, что Г. под видом представителя Группы компаний «Профит Групп», расположенной на территории г. Самары, путем обмана и злоупотребления доверием, под предлогам оказания брокерских услуг на внебирже-

[1] Письмо ГСУ ГУ МВД России по Московской области от 08.08.2019 № 14/7993.

вой валютой торговой площадке «Forex» В., открытия ей торговых счетов для осуществления сделок купли-продажи иностранной валюты побудил последнюю, с использованием платежной системы «Яндекс.Деньги», внести денежные средства в осумме 530 392 рублей на виртуальные счета компаний «Profit Group International S.A.» и «Profit Asset Management LTD».

В ходе проведенных обысков по месту жительства и работы обвиняемого была изъята компьютерная техника, которая осмотрена специалистом, а также проведена компьютерная судебная экспертиза. В ходе осмотра компьютерной техники установлено, что денежные средства на счета компаний «Profit Group International S.A.h, «Profit Asset Management LTD» не поступали, а были перечислены на счет открытого акционерное общество «Приор Банк», расположенного в Республике Беларусь, а также на территории Республик Кипр и Панамы, в связи с чем в соответствии с международным законодательством в указанные выше республики были направлены запросы об оказании правовой помощи в части изъятия бухгалтерских и финансовых документов на основании судебного решения, полученного на территории Российской Федерации в соответствии со ст. 183 УПК РФ, которые были предоставлены на электронных носителях. В дальнейшем электронные носители были осмотрены с участием специалиста, признаны вещественным доказательством по уголовному делу и в соответствии с требованиями п. «а» ч. 5 ст. 82 УПК РФ хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации[1].

Таким образом, изъятые в ходе расследования указанных уголовных дел электронные носители информации использованы органами предварительного следствия как неоспоримые доказательства.

Приговором Конаковского городского суда Тверской области от 02.04.2019 К. признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 273 и ч. 4 ст. 159.6 УК РФ, и приговорен к 3 годам 6 месяцам лишения свободы с отбыванием наказания в исправительной колонии общего режима[2].

Большое количество криминалистически значимой информации содержат социальные сети, развитие которых на протяжении ряда лет претерпевает бурный рост. Социальные сети используются как для общения, знакомств, формирования сообществ с близкими

[1] Письмо ГСУ ГУ МВД России по Самарской области от 10.07.2019 № 12/37-8947.
[2] Письмо ГСУ ГУ МВД России по Московской области от 08.08.2019 № 14/7993.

интересами, так и для распространения новостей, маркетингового продвижения товаров, работ, услуг и, наконец, просто развлечения. В настоящее время наиболее крупными по охвату аудитории русскоязычными социальными сетями являются «ВКонтакте» и «Одноклассники». Широкое распространение в России получили также Instagram, Facebook, Twitter. Анализ контента, который выкладывают пользователи социальных сетей на свои страницы, сети позволяет определить круг общения пользователя, его образ жизни, увлечения, способы проведения досуга, род занятий, уровень доходов, географию перемещений, семейное положение и состав семьи, используемый автотранспорт, а также иные сведения, имеющие значение при выдвижении и проверке следственных версий.

Несмотря на то, что пользователи социальных сетей имеют возможность не указывать при регистрации свои подлинные персональные данные, а использовать псевдоидентификаторы: аватар (графическое изображение, произвольно выбранное пользователем социальной сети или интернет-ресурса для самоидентификации), никнейм (сетевое имя, псевдоним, используемый для общения анонимных пользователей), существуют возможности для их деанонимизации. При регистрации в социальной сети каждому пользователю присваивается персональный идентификатор, для получения которого ему необходимо указать актуальный номер сотового телефона, на который при поступает SMS-сообщение с кодом подтверждения. При этом правилами оказания услуг связи, принимаемыми Правительством Российской Федерации на основании ст. 44 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», на оператора связи возложена обязанность идентификации пользователей услугами связи по передаче данных и предоставлению доступа к сети Интернет и используемого ими оконечного оборудования. Соответственно, оператор связи обязан располагать достоверными сведениями о своих абонентах. При этом они обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность, хранящуюся у них информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами. Постановлением Правительства Российской Федерации от 31.07.2014 № 759 определен состав информации, подлежащей хранению в соответствии с названными требованиями, место и правила ее хранения, порядок ее предоставления уполномоченным государственным органам.

Важно отметить, что на основании пп. 2 п. 3 ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» организатор распространения информации в сети Интернет обязан хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение трех лет;

2) текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео- и иные электронные сообщения пользователей сети Интернет в течение шести месяцев.

Соответственно, при наличии достаточных оснований полагать, что информация, содержащаяся в социальных сетях, может иметь доказательственное значение, следователь вправе поручить органу дознания, осуществляющему оперативно-розыскное сопровождение расследования, получить в организации, осуществляющей администрирование социальной сети или в ее российском представительстве, сведения, указанные выше.

Заметим, что названный объем сведений, сроки их хранения и порядок получения в равной степени применим и к иным распространенным интернет-сервисам: электронной почте, сервисам мгновенных сообщений (мессенджерам) и др. Организации, администрирующие указанные ресурсы, располагают персональными данными пользователей, указанными ими при регистрации, информацией о дате и времени регистрации, IP-адресе доступа к сети Интернет при регистрации, абонентском номере сотовой связи (для SMS-подтверждения), продолжительности использования учетной записи и иные сведения[1]. Кроме того, возможно получение сведений о произведенных в социальной сети платежных операциях и переписке пользователя, однако для этого требуется судебное решение, поскольку данная информация относится к охраняемой законом тайне.

[1] Полный перечень информации, подлежащей хранению организатором распространения информации в сети Интернет, к числу которых относятся и социальные сети, предусмотрен п. 3 Правил хранения организаторами распространения информации в информационно-телекоммуникационной сети Интернет информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети Интернет и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 31.07.2014 № 759.

Анализ содержащихся в социальных сетях данных о контактах фигурантов преступлений позволяет установить соучастников, выявить ранее не установленных свидетелей и потерпевших, выявить внутреннюю структуру преступной организации, роль отдельных ее членов, а также иные сведения, имеющие значение для дела.

Следует отметить, что в настоящее время разработаны и применяются специализированные программные комплексы, позволяющие осуществлять поиск и систематизацию информации из общедоступных онлайн источников (включая и социальные сети, форумы, блоги и т. п.) с использованием семантических фильтров, позволяющих четко систематизировать информацию и избавить ее от «информационного шума»[1].

В связи с тем, что электронная почта нередко используется как средство коммуникации при подготовке, совершении и сокрытии преступлений, переписка, осуществляемая с использованием данного интернет-сервиса, представляет собой весьма важный источник криминалистически значимой информации.

При этом процессе обнаружения, фиксации отправлений электронной почты следует учитывать следующие технологические особенности данного сервиса: сообщения электронной почты могут сохраняться на персональном компьютере отправителя и получения электронной почты, на серверах программ получения / отправки электронной почты (mail.ru, gmail.com, yandex.ru и др), а также провайдера, предоставляющего услуги связи. Представляет интерес следующая криминалистически значимая информация, которую можно получить в организациях, осуществляющих администрирование данных информационных ресурсов: данные учетной записи (аналогично социальным сетям), даты и время доступа к электронному почтовому ящику, произведенные изменения в учетной записи (смена пароля, изменение телефона, контрольного вопроса и пр.), перечень контактов пользователя и содержание его переписки.

Перечисленная информация может быть получена не только от российских организаций – собственников сервисов электронной почты, но и от организаций, зарегистрированных вне юрисдикции Российской Федерации, но имеющих на территории страны свои представительства.

Использование в противоправной деятельности сервисов перевода электронных денежных средств[2] (Яндекс.Деньги», «QIWI-

[1] Примером подобных программных комплексов является «ЛКС Аналитика», «СПРУТ», «Крибрум», «Катюша», «Зеус», «Лисс-М», «Буратино», «Доктор Ватсон», «Демон Лапласа» и др.

[2] Электронные денежные средства – денежные средства, которые предварительно предоставлены одним лицом другому лицу, учитывающему информацию о размере

кошелек», «WebMoney» и т. п.) значительно облегчают совершение финансовых транзакций, при этом предоставляет широкие возможности для установления персональных данных лиц, которые прошли процедуру идентификации в соответствии с требованиями Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а именно: фамилия, имя и отчество лица, на чье имя зарегистрирован электронный кошелек; дата и место его рождения; гражданство; реквизиты документа, удостоверяющего личность; адрес места жительства; идентификационный номер налогоплательщика; номера телефонов; место работы и должность; цели финансово-хозяйственной деятельности, финансовое положение, деловая репутация, источники происхождения денежных средств и (или) иного имущества и др.

Использовать сервисы перевода электронных денежных средств физические лица могут и без осуществления процедуры идентификации. В этом случае предельно допустимый остаток на балансе таких лиц не может превышать 15 000 руб., платежи можно осуществить на сумму до 40 000 руб. в месяц, а снятие наличных не может превышать 5 000 руб. в день и 20 000 руб. в месяц.

В организациях, оказывающих услуги по переводу электронных денежных средств, возможно получение информации о сеансах доступа к учетной записи (электронному кошельку) за определенный период времени, а также данные систем видеорегистрации терминалов оплаты.

Таким образом, в сети Интернет, а также в организациях, оказывающих услуги интернет-сервисов, содержится значительный массив криминалистически значимой информации, эффективное использование которой позволяет существенно повысить качество расследования преступлений экстремистской направленности, вооружает органы расследования преступлений дополнительным инструментарием, обеспечивающим формирование достаточной доказательственной базы при осуществлении уголовного преследования лиц, совершивших преступление.

Помимо социальных сетей, электронной почты, мессенджеров и платежных систем для выдвижения и проверки следственных версий, а также получения фактических оснований для последующего производства следственных действий существенным инфор-

---

предоставленных денежных средств без открытия банковского счета, для исполнения денежных обязательств перед третьими лицами, и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа (см.: п. 18 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»).

мационным ресурсом являются открытые данные государственных органов, органов местного самоуправления и организаций, осуществляющих отдельные государственные полномочия. Открытые данные МВД России, Министерства юстиции РФ, ФНС, ФССП, Росреестра, Росфинмониторинга, Банка России, Судебного департамента при Верховном Суде, Генеральной прокуратуры Российской Федерации, иных государственных органов позволяют производить поиск судебных решений, проверку действительности паспортов, разрешений на работу и патентов на осуществление трудовой деятельности, приглашений на въезд в Российскую Федерацию иностранных граждан и лиц без гражданства, наличия оснований для неразрешения въезда на территорию Российской Федерации иностранным гражданам и лицам без гражданства по линии МВД России, получать подробную информацию о юридических лицах и индивидуальных предпринимателях, данные исполнительных производств, сведения об объектах недвижимости, в том числе с визуализацией на публичной кадастровой карте, уведомления о залоге движимого имущества, реестр наследственных дел, сведения о статусе кредитных, микрофинансовых, страховых организаций и негосударственных пенсионных фондов, реестры государственных и муниципальных закупок, недобросовестных поставщиков, сведения о деятельности некоммерческих организаций, организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, и многое другое.

Криминалистически значимую информацию содержат и иные интернет-сервисы, позволяющие решать поисково-познавательные задачи, возникающие в процессе расследования. Так, сервис yandex.ru/people позволяет осуществлять поиск личных страниц социальных в сетях по имени, фамилии или «никнейму». Сходным функционалом обладает сервис pipl.com. Сервис SocialSearcher помогает найти последние сообщения определенного пользователя в социальных сетях. Сервис Sounds осуществляет анализ и распознавание звуков или их сочетаний в аудиопотоке, распознает голоса и преобразует в текст. Сервис 2ip.ru позволяют установить IP-адрес отправителя электронной почты. Сервис whois позволят интернет-провайдера, предоставившего соответствующий IP-адрес, также узнать регистрационную информацию о домене. Сервис https://archive.org/web/ позволяет производить поиск и просмотр удаленных web-страниц.

В целях комплексного поиска информации одновременно по нескольким открытым источникам используются метапоисковые системы, предоставляюшие дополнительный инструмента-

рий решения информационно-аналитических задач, возникающих в процессе раскрытия и расследования преступлений, в частности, таких как:

– установление связей, интересов, предпочтений, психологических особенностей конкретного лица, его биографических событий, места работы жительства, транспортных средствах и пр.;

– систематизация контактов лица по различным основаниям: активность, локация, способ связи, характер взаимодействия, региональная принадлежность и пр.;

– оценка финансового состояния организации на основе анализа его отчетности;

– выявление признаков аффилированности лиц и организаций на основе информации об учредителях, руководителях, конечных бенефициарах;

– выявление недобросовестной «миграции» организации с целью уклонения от выполнения договорных обязательств;

– отслеживание истории участия организации в государственных и муниципальных закупках;

– анализ публикаций в СМИ и интернет-ресурсах;

– выявление существенных фактов (изменение регистрационных данных, смена учредителя / руководителя, планируемые процедуры ликвидации, реорганизации или банкротства, судебные дела и др.).

– выявление источников финансирования преступной деятельности на основе построения графа связей руководителей и учредителей юридического лица; и др.

Проведенное исследование показало, что использование в практической деятельности органов предварительного следствия средств комплексного получения информации государственных и муниципальных информационных систем, а также открытых интернет-ресурсов для получения криминалистически значимой информации, необходимой при выдвижении и проверке следственных версий, используется недостаточно и носит, скорее, исключительный характер. Вместе с тем, совместное использование открытых данных государственных органов и интегрированных банков данных органов внутренних дел способно вывести уровень информационного обеспечения органов предварительного следствия на качественно новый уровень.

Следует отметить, что согласно требованиям действующего законодательства в сфере информации, связи, финансовой и банковской деятельности при совершении того или иного действия с использованием сервисов сети Интернет образуются цифровые

следы, позволяющие установить лицо, совершившее противоправное деяние, и установить обстоятельства его совершения.

Так, на основании ст. 44 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» услуги подвижной радиотелефонной (сотовой) связи предоставляются только тем абонентам (физическим и юридическим лицам, а также индивидуальным предпринимателям), достоверные сведения о которых предоставлены оператору связи в соответствии с правилами оказания услуг связи. Последние определяют порядок идентификации пользователей услугами связи по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети Интернет и используемого ими оконечного оборудования.

Согласно ст. 64 указанного Федерального закона и ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» операторы связи и организаторы распространения информации в сети Интернет обязаны хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений, а также сами вышеуказанные сообщения.

Федеральный закон от 29.07.2017 № 241-ФЗ обязывает организатора обмена мгновенными сообщениями (мессенджеров) обеспечивать идентификацию своих клиентов (с использованием абонентского номера, на основании соответствующего договора), а также в течение суток с момента получения соответствующего требования уполномоченного органа ограничить возможность осуществления пользователем сервиса обмена сообщениями и хранить идентификационные сведения об абонентском номере только на территории РФ.

Федеральным законом от 05.05.2014 № 110-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» ограничены возможности совершения анонимных онлайн-платежей и определен порядок идентификации клиентов при совершении платежей свыше 15 000 руб. В процессе идентификации подлежит фиксации фамилия, имя, а также отчество, гражданство, дата рождения, реквизиты документа, удостоверяющего личность и иные данные плательщика.

Положение Банка России от 09.06.2012 № 382-П устанавливает перечень сведений, подлежащих фиксации оператором электронных платежных средств, включая данные о совершенных переводах денежных средств, об остатках электронных денежных средств и осуществленных переводах, включая точное время (с точностью до секунды) осуществления платежа, информацию об устройстве, с использованием которого осуществлен доступ к автоматизирован-

ной системе, используемое программное обеспечение, IP-адрес входа в сеть Интернет, MAC-адрес сетевого оборудования, номер SIM-карты, номер телефона и (или) иной идентификатор устройства.

На основании ст. 26 Закона Российской Федерации от 02.12.1990 № 395-1 «О банках и банковской деятельности» справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, а при наличии согласия руководителя следственного органа – органам предварительного следствия по делам, находящимся в их производстве.

Приведенные положения действующего законодательства формируют правовую основу обнаружения, фиксации и изъятия цифровых следов, возникающих в процессе совершения и сокрытия преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Вопросы для повторения

1. Социальные сети как источники криминалистически значимой информации.
2. Сервисы электронной почты и мессенджеры как источники криминалистически значимой информации.
3. Платежные системы и системы дистанционного банковского обслуживания как источники криминалистически значимой информации.

Практическое задание

Используя открытые источники данных, установить факты участия организаций, учредителем (руководителем) которых является гр. ... (персональные данные) в государственных и муниципальных закупках.

Заключение

Изменения, произошедшие в жизнедеятельности граждан и организаций в связи с проведением мероприятий по ограничению распространения новой коронавирусной инфекции COVID-19, проявились в смене привычного ритма жизни, переводе на удаленную работу, введении режима самоизоляции, ограничений на свободу передвижения, приостановлении деятельности ряда организаций сферы услуг, организации досуга и пр.

С другой стороны, перечисленные ограничения придали колоссальный импульс дальнейшему развитию цифровых технологий и их интенсивной интеграции в образовательную деятельность, финансовый сектор, а также ряд других сфер социально-экономической деятельности. В этих условиях усилилась зависимость как всего общества в целом, так и отдельных лиц от бесперебойного функционирования сервисов оказания государственных услуг в электронной форме, систем дистанционного банковского обслуживания, каналов связи и иной информационной инфраструктуры. Повседневная деятельность большинства организаций стала осуществляться на основе коммуникаций посредством электронной почты, сервисов видеоконференцсвязи и облачных хранилищ данных. На дистанционный режим работы перешли целые сектора экономики. При таких обстоятельствах кратно возросли риски, связанные с негативными последствиями противоправных посягательств на цифровые данные, вызванные преступлениями, совершенными с использованием информационно-телекоммуникационных технологий, рост которых является не только российской, но и общемировой тенденцией.

С учетом сказанного потребность в научно обоснованных рекомендациях относительно порядка собирания, проверки и оценки и использования доказательств на электронных носителях информации будет только нарастать. Представляют высокую актуальность вопросы обнаружения, фиксации и изъятия информации о транзакциях с использованием криптовалют, преодоления средств анонимизации пользователей в сети Интернет, а также использования иных цифровых технологий в противоправной деятельности. С этой связи исследования в данном направлении будут продолжены.

Рекомендуемая литература

Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г.) // Собр. законодательства Рос. Федерации. 2014. № 31. Ст. 4398.

Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня1996 г. № 63-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

Уголовно-процессуальный кодекс РСФСР: утв. ВС РСФСР 27.10.1960 // Рос. газ. 2001. 31 декабря.

О социальной защите граждан, подвергшихся воздействию радиации вследствие катастрофы на Чернобыльской ГАЭС: Закон РФ от 15 мая 1991 г. № 1244-1 // Доступ из справ.-правовой системы «КонсультантПлюс».

О банках и банковской деятельности: Закон РФ от 2 декабря 1990 г. № 395-1 // Доступ из справ.-правовой системы «КонсультантПлюс».

О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 5 мая 2014 г. № 110-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

Об Оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144- ФЗ // Собр. законодательства Рос. Федерации. 1995. № 33. Ст. 3349.

О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

Об электронной цифровой подписи: Федеральный закон от 10 января 2002 г. № 1-ФЗ // Собр. законодательства Рос. Федерации. 2002. № 2. Ст. 127.

О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента Российской Федерации от 7 мая 2018 г. № 204 // Доступ из справ.-правовой системы «КонсультантПлюс».

О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Доступ из справ.-правовой системы «КонсультантПлюс».

О Стратегии научно-технологического развития Российской Федерации: указ Президента Российской Федерации от 1 декабря 2016 г. № 642 // Доступ из справ.-правовой системы «КонсультантПлюс».

Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Доступ из справ.-правовой системы «КонсультантПлюс».

Расширенная коллегия МВД России [Электронный ресурс]. URL: http://www.kremlin.ru/catalog/persons/310/events/65090 (дата обращения: 04.03.2021).

Алиев Т. Т., Громов Н. А., Макаров Л. В. Уголовно-процессуальное доказывание. Москва, 2002.

Алексеев Н. С., Даев В. Г., Кокорев Л. Д. Очерк развития науки советского уголовного процесса. Воронеж, 1980.

Арсеньев В. Д. Вопросы общей теории судебных доказательств. Москва, 1964.

Афанасьев В. Г. Социальная информация и управление обществом. Москва, 1975.

Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. ... канд. юрид. наук. Москва, 2020.

Баршев Я. И. Основания уголовного судопроизводства с применением к российскому уголовному судопроизводству. Москва: ЛексЭст, 2001.

Бедняков Д. И. Непроцессуальная информация и расследование преступлений. Москва, 1991.

Белкин А. Р. Теория доказывания в уголовном судопроизводстве. Москва: Норма, 2005.

Белкин Р. С. Криминалистическая энциклопедия. 2-е изд., доп. Москва: Мега-трон XXI, 2000.

Белкин Р. С. Собирание, исследование и оценка доказательств. Сущность и методы. Москва: Наука, 1966.

Бирюков Б. В. Кибернетика и методология науки. Москва, 1974.

Винер Н. Кибернетика и общество. Москва, 1958.

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

Владимиров Л. Е. Учение об уголовных доказательствах. Тула: Автограф, 2000.

Ворожбит С. П. Электронные средства доказывания в гражданском и арбитражном процессе: автореф. дис. ... канд. юрид. наук: 12.00.05. Санкт-Петербург, 2011.

Гаврилин Ю. В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: монография. Тула, 2009.

Гаврилин Ю. В. Организационно-методическое обеспечение расследования преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации // Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: в 2 ч. Москва: Академия управления МВД России, 2019. Ч. 1.

Гаврилин Ю. В. Криминалистические особенности обнаружения, фиксации, изъятия и исследования электронных следов преступления // Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: в 2 ч. / А. В. Аносов [и др.]. Москва: Академия управления МВД России, 2019. Ч. 1.

Галяшина Е. И. Теоретические и прикладные основы судебной фоноскопической экспертизы: автореф. дис. ... д-ра юрид. наук. Воронеж, 2002.

Громов Н. А., Пономаренков В. А., Гущин А. Н., Францифоров Ю. В. Доказательства, доказывание и использование результатов оперативно-розыскной деятельности. Москва, 2001.

Горский Г. Ф., Кокорев Л. Д., Элькинд П. С. Проблемы доказательств в советском уголовном процессе. Воронеж: изд-во Воронеж. ун-та, 1978.

Грибунов О. П., Старичков М. В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие. Иркутск: ФГКОУ ВПО ВСИ МВД России, 2014.

Громов Н. А., Зайцева С. А., Гущин А. Н. Доказательства: их виды и доказывание в уголовном процессе. Москва, 2006.

Духовской М. В. Русский уголовный процесс. Москва, 1910.

Згадзай О. З., Казанцев С. Я., Филиппов А. В. Информатика и математика для юристов: учебник. Казань, 2000.

Земцова С. И. Методика расследования незаконного сбыта наркотических средств, совершенного с использованием интернет-технологий: учебное пособие / С. И. Земцова, О. А. Суров, П. В. Галушин. Москва: Юрлитинформ, 2019.

Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: дис. ... канд. юрид. наук. Челябинск, 2010.

Иванов Е. Е. Уведомление в досудебных стадиях уголовного судопроизводства: автореф. дис. ... канд. юрид. наук. Москва, 2020.

Игнатьев Д. Б. Документы как доказательства по делам о налоговых преступлениях: автореф. дис. ... канд. юрид. наук. Волгоград, 2001.

Карев Я. А. Электронные документы и сообщения в коммерческом обороте. М., 2006.

Карнеева Л. М. Доказательства и доказывание в уголовном процессе: учебное пособие. Москва: УМЦ при ГУК МВД РФ, 1994.

Кипнис Н. М. Допустимость доказательств в уголовном судопроизводстве. Москва, 1995.

Кокорев Л. Д., Кузнецов Н. П. Уголовный процесс: доказательства и доказывание. Воронеж, 1995.

Кореневский Ю. В., Падва Г. П. Участие защитника в доказывании по новому уголовно-процессуальному законодательству. Москва, 2004.

Костенко Р. В. Понятие и признаки уголовно-процессуальных доказательств. Москва: Юрлитинформ, 2006.

Лазарева В. А. Доказывание в уголовном процессе: учебно-практическое пособие. Москва: Высшее образование, 2009.

Ланцман Р. М. Использование возможностей кибернетики в криминалистической экспертизе и некоторые проблемы уголовно-судебного доказывания: автореф. дис. ... д-ра юрид. наук. Москва, 1970.

Леви А. А. Звукозапись в уголовном процессе. Москва, 1974.

Митрофанова М. А. Электронные доказательства и принципы непосредственности в арбитражном процессе: дис. ... канд. юрид. наук. Саратов, 2013.

Овчинский А. С. Информация и оперативно-розыскная деятельность. Москва, 2002.

Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. Москва, 2008.

Орлов Ю. К. Основы теории доказательств в уголовном процессе: научно-практическое пособие. Москва: Проспект, 2000.

Панфилов П. О. Особенности производства по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности: автореф. дис. ... канд. юрид. наук. Москва, 2019.

Победкин А. В. Уголовно-процессуальное доказывание. Москва: Юрлитинформ, 2009.

Победкин А. В., Яшин В. Н. Следственные действия. Москва: Юрлитинформ, 2016.

Першиков В. И., Савинков В. М. Толковый словарь по информатике. Москва: Финансы и статистика, 1991.

Семенцов В. А. Видео- и звукозапись в доказательственной деятельности следователя: дис. ... канд. юрид. наук. Екатеринбург, 1994.

Семенцов В. А. Следственные действия в досудебном производстве (общие положения теории и практики): монография. Екатеринбург, 2006.

Сенкевич Г. Е. Искусство восстановления данных. Санкт-Петербург: БХВ-Петербург, 2011.

Строгович М. С. Избранные труды. Москва, 1991. Т. 3.

Строгович М. С. Курс советского уголовного процесса. Москва, 1958.

Строгович М. С. Теория доказательств в советском уголовном процессе. Москва: Юр. лит., 1966–1967: в 2-х т.

Трусов А. И. Основы теории судебных доказательств. Москва: Госюриздат, 1960.

Урсул А. Д. Проблемы информации в современной науке. Философские очерки. Москва, 1975.

Фаткуллин Ф. Н. Общие проблемы процессуального доказывания. Казань, 1976.

Фойницкий И. Я. Курс уголовного судопроизводства. Санкт-Петербург, 1996. Т. 2.

Чельцов М. А. Советский уголовный процесс. Москва, 1962.

Шейфер С. А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования. Тольятти, 1998.

Шейфер С. А. Собирание доказательств в советском уголовном процессе. Саратов, 1986.

Информационная безопасность и защита информации: сборник терминов и определений. Москва, 2001.

Курс советского уголовного процесса: общая часть / под ред. А. Д. Бойкова и И. И. Карпеца. Москва, 1989.

Правовая кибернетика социалистических стран: учебное пособие / под ред. Н. С. Полевого. Москва, 1987.

Собрание узаконений и распоряжений Рабочего и Крестьянского правительства. Москва, 1918. № 53.

Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. 2-е изд., испр., и доп. Москва: Юрид. лит., 1973.

Уголовно-процессуальное право Российской Федерации: учебник / отв ред. П. А. Лупинская. Москва, 2003.

Учение об уголовных доказательствах. Части: Общая и Особенная / Л. Е. Владимиров. 3-е изд., изм. и законч. Санкт-Петербург, 1910.

Энциклопедия «Касперского». Хэширование: сайт. URL: https://encyclopedia.kaspersky.ru/glossary/hashing/ (дата обращения: 15.03.2020).

Энциклопедия «Касперского». MD5: сайт. URL: https://encyclopedia.kaspersky.ru/glossary/md5/ (дата обращения: 15.03.2020).

ДЛЯ ЗАМЕТОК

Учебное издание

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ, В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ

Учебное пособие

Редактор *Д. В. Алентьев*
Корректор *А. А. Уварова*
Верстка *С. Н. Портнова*

Подписано в печать 02.06.2021. Формат 60 × 84 $^{1}/_{16}$.
Усл.печ. л. 6,62. Уч.-изд. л. 8,14. Тираж 94 экз. Заказ № _

Отделение полиграфической и оперативной печати РИО
Академии управления МВД России
125993, Москва, ул. Зои и Александра Космодемьянских, д. 8