УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ

ИСПОЛЬЗОВАНИЕ В ДОКАЗЫВАНИИ ИНФОРМАЦИИ, ПРЕДОСТАВЛЕННОЙ В ЭЛЕКТРОННОМ ВИДЕ (ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ)

УЧЕБНОЕ ПОСОБИЕ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИСПОЛЬЗОВАНИЕ В ДОКАЗЫВАНИИ ИНФОРМАЦИИ, ПРЕДОСТАВЛЕННОЙ В ЭЛЕКТРОННОМ ВИДЕ (ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ)

Учебное пособие

Уфа 2024

УДК 343.140.28:004.63.087(470)(075.8)
ББК 67.410.204.19с517(2Рос)я73-1
И88

Рекомендовано к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России

Рецензенты:
кандидат юридических наук, доцент Д. Н. Рудов
(Белгородский юридический институт МВД России имени И. Д. Путилина);
кандидат юридических наук, доцент С. М. Кузнецова
(Дальневосточный юридический институт МВД России
имени И. Ф. Шилова)

Коллектив авторов:
Р. Р. Абдразяпов – кандидат юридических наук, б/з;
А. Р. Арсланова – кандидат юридических наук, б/з;
С. С. Телигисова – кандидат педагогических наук, б/з;
М. А. Нуров – б/с, б/з

И88 **Использование в доказывании информации, предоставленной в электронном виде (вопросы теории и практики)** : учебное пособие / Р. Р. Абдразяпов, А. Р. Арсланова, С. С. Телигисова, М. А. Нуров. – Уфа : Уфимский ЮИ МВД России, 2024. – 64 с. – Текст : непосредственный.

ISBN 978-5-7247-1184-5

В учебном пособии рассматриваются теоретические и правовые аспекты получения доказательств и информации в связи с обнаружением или возможностью обнаружения электронных носителей. Авторы комплексно анализируют проблемы использования информации, представленной в электронном виде, в качестве доказательств в уголовном процессе; рассматривают особенности правового режима доказательственной информации в электронном виде; анализируют действующий процессуальный порядок собирания доказательственной информации на электронных носителях, а также ее проверки и оценки.

Издание предназначено для обучающихся образовательных организаций МВД России, сотрудников органов, организаций, подразделений МВД России.

УДК 343.140.28:004.087(470)(075.8)
ББК 67.410.204.19с517(2Рос)я73-1

ISBN 978-5-7247-1184-5

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ…… 4

ГЛАВА 1. ПРАВОВАЯ ПРИРОДА ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ПРЕДСТАВЛЕННОЙ В ЭЛЕКТРОННОМ ВИДЕ….. 6
§ 1. Информация, представленная в электронном виде, в системе доказательств по уголовному делу……. 6
§ 2. Правовой режим доказательственной информации, представленной в электронном виде……... 13
§ 3. Законодательные и правоприменительные аспекты получения сведений приватного характера при формировании предмета доказывания по преступлениям, совершенным с использованием современных цифровых и компьютерных технологий…….. 17

ГЛАВА 2. ПРОБЛЕМЫ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИИ, ПРЕДСТАВЛЕННОЙ В ЭЛЕКТРОННОМ ВИДЕ, В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВА ПО УГОЛОВНОМУ ДЕЛУ…….. 29
§ 1. Собирание доказательственной информации, представленной в электронном виде, в ходе следственных действий…….. 29
§ 2. Особенности назначения и производства экспертиз электронных носителей информации……. 43
§ 3. Проблемные вопросы проверки и оценки информации, представленной в электронном виде, в качестве доказательства……. 47

ЗАКЛЮЧЕНИЕ…….. 50

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ…… 56

ВВЕДЕНИЕ

В современных реалиях повсеместной цифровизации и глобальной информатизации общества, всплеска предоставления услуг в сфере высоких информационно-телекоммуникационных технологий проникновение различных электронных устройств в повседневный социум приобретает важное значение и получает широкое распространение.

Не обошел этот процесс и действующее уголовно-процессуальное законодательство. Современным уголовно-процессуальным отношениям свойственно постоянно расширяющееся использование информационно-телекоммуникационных технологий. Данный процесс характерен как для криминальной стороны жизни, так и для деятельности правоохранительных органов, противодействующих преступности. В таких условиях остро встает вопрос использования информации, представленной в электронном виде (электронных доказательств), в уголовном судопроизводстве, ее правового режима и уголовно-процессуальной формы.

Необходимость исследования особенностей использования информации, представленной в электронном виде, в качестве доказательств в уголовном процессе, проблем ее правового регулирования обусловлена потребностями практики, которая все чаще использует сведения из электронных источников, непосредственно сами электронные носители информации в процессе доказывания.

Кроме того, порядок обращения с электронными доказательствами в действующем уголовно-процессуальном законодательстве не находит должного правового регулирования, тогда как институт уголовно-процессуального доказывания сталкивается с появлением новых способов сбора, использования, оценки и хранения информации, представленной в электронном виде. В подобных условиях необходимо детальное правовое закрепление условий, порядка и последствий использования доказательственной информации по уголовным делам, представленной в электронном виде, чтобы минимизировать ошибки правоприменения на практике.

Несмотря на отмеченную тенденцию постоянного расширения использования информации, представленной в электронном виде, в качестве доказательств, в уголовно-процессуальном законе отсутствует определения таких понятий, как электронный носитель информации, электронное доказательство, четко не закреплен процессуальный порядок получения доказательственной информации на электронных носителях. Указанные недостатки напрямую влияют на качество, результативность предварительного расследования уголовных дел, не дают возможность правильно собрать и оформить доказательства в виде информации на электронных носителях.

Помимо вышеперечисленных, немало проблем возникает в процессе установления и сохранения подлинности и целостности доказательственной информации, представляемой в электронном виде, поскольку такие данные достаточно уязвимы.

Сказанное обуславливает актуальность темы издания, необходимость дальнейшего научного осмысления проблем использования информации, представленной в электронном виде.

ГЛАВА 1. ПРАВОВАЯ ПРИРОДА ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ПРЕДСТАВЛЕННОЙ В ЭЛЕКТРОННОМ ВИДЕ

§ 1. Информация, представленная в электронном виде, в системе доказательств по уголовному делу

Непрерывное развитие информационных технологий и их распространение во всех сферах жизни современного общества, в том числе и в сфере уголовного судопроизводства, требуют разъяснений положений закона, касающихся вопросов использования в доказывании по уголовным делам информации, представленной в электронном виде. Анализ уголовно-процессуального законодательства и практики его применения показывает, что в реальности правоприменители при использовании информации, представленной в электронном виде, сталкиваются с большим количеством спорных, проблемных моментов, требующих осмысления, обоснования и практической реализации.

Электронная информация, используемая в качестве доказательства в уголовном процессе, может быть представлена в виде электронных документов, писем или других файлов, а также записей, хранящихся сетевыми или интернет-провайдерами.

Уголовно-процессуальный кодекс Российской Федерации[1] (далее – УПК РФ) доказательствами по уголовному делу признает «любые сведения, на основе которых устанавливается наличие или отсутствие подлежащих доказыванию при производстве по уголовному делу обстоятельств, а также иных имеющих значение для уголовного дела обстоятельств» (ст. 74). Также уголовно-процессуальный закон содержит перечень доказательств, к числу которых относится категория «иные документы».

Несмотря на широкое использование в доказывании информации, представленной в электронном виде, УПК РФ не дает определения понятию «электронный носитель информации». Указанный недостаток нормативного регулирования отрицательно сказывается на качестве деятельности органов предварительного расследования, которая по большей части является правоограничительной, а значит, не допускает вольной трактовки понятий, которые в той или иной степени затрагивают права и свободы участников уголовного процесса.

Согласно п. 3.28 ГОСТ Р 7.0.95-2015 «Система стандартов по информации, библиотечному и издательскому делу. Электронные документы. Основные виды, выходные сведения, технологические характеристики» электронный носитель информации (электронный носитель данных) –

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Российская газета. 2001. № 249.

это материальный объект, используемый для записи, хранения и воспроизведения цифровой информации[1].

Согласно Федеральному закону от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» «электронное средство платежа – это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей и информации, в том числе платежных карт, а также иных технических устройств (п. 19)»[2].

По мнению С. Ю. Скобелина, «к электронным носителям информации следует относить компьютер, моноблок, ноутбук, планшет, мобильные устройства (телефоны, смартфоны), с помощью которых можно получить информацию, интересующую правоохранительные органы: записи телефонной книги, сообщения, контакты в электронной почте, переписку в социальных сетях, изображения; аудио и видео-файлы»[3].

Как отмечает Ю. Н. Соколов, «под электронным носителем информации следует понимать технически и технологически адаптивное 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»[4]. По мнению автора, к данным объектам можно отнести мобильные телефоны, планшеты, ноутбуки, системные блоки и т. д.

По мнению В. Н. Григорьева и О. А. Максимова: «в связи с тем, что в законодательстве отсутствует определение «электронный носитель информации», толкование термина должно быть обоснованным и узким, чтобы не допустить отнесения к рассматриваемому термину, к примеру, мобильного телефона, для изъятия которого следователю (дознавателю) не требуется специальных знаний»[5].

---

[1] ГОСТ Р 7.0.95-2015. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Электронные документы. Основные виды, выходные сведения, технологические характеристики (утв. и введен в действие приказом Росстандарта от 9 декабря 2015 г. № 2127-ст). М. : Стандартинформ, 2017.

[2] О национальной платежной системе : федеральный закон Российской Федерации от 27 июня 2011 г. № 161-ФЗ // Российская газета. 2011. № 139.

[3] Скобелин С. Ю. Использование специальных знаний при работе с электронными следами // Российский следователь. 2019. № 20. С. 32.

[4] Соколов Ю. Н. Электронный носитель информации в уголовном процессе // Информационное право. 2019. № 3. С. 22.

[5] Григорьев В. Н., Максимов О. А. Некоторые вопросы использования электронных носителей информации при расследовании уголовных дел // Полицейская деятельность. 2018. № 1. С. 16.

Отсутствие законодательного определения понятия «электронный носитель информации» не позволяет единообразно и четко определить его сущность, а также перечень объектов, относящихся к нему, что в конечном итоге затрудняет практику применения электронных носителей информации в доказывании по уголовным делам. По мнению Ю. В. Гаврилина: «следует сформулировать определение термина так, чтобы исключить на практике его произвольную интерпретацию и подмену. Добиться этого возможно не техническим описанием понятия, а указанием на значимую для дела составляющую таких источников доказательств»[1]. Данное высказывание имеет свою практическую значимость, однако если речь идет об электронном носителе и он уже выделяется законодателем в отдельную категорию, то все же технические понятия должны учитываться при производстве процессуальных и следственных действий.

Обобщив информацию по исследуемой тематике, мы придерживаемся того, что основными признаками, которыми должны обладать электронный носитель информации и информация, на нем содержащаяся, чтобы их можно было применить в качестве доказательства по уголовному делу, являются:

– значимость информации для расследования конкретного уголовного дела;

– достоверность источника, из которого получена информация (возможность проверки данного источника);

– доступность информации для восприятия участниками процесса (видеозапись, скриншот сайтов и т. д.);

– изъятие электронного носителя информации в строгом соответствии с уголовно-процессуальным порядком, закрепленным действующим законодательством.

Споры среди ученых-процессуалистов вызывает вопрос о месте электронных носителей информации в системе доказательств по уголовным делам. Это связано с тем, что уголовно-процессуальный закон не относит их к какому-либо конкретному источнику доказательств из перечня, указанного в ч. 2 ст. 74 УПК РФ. По мнению одних ученых, электронные носители информации следует относить к иным документам, по мнению других – к вещественным доказательствам. Третья группа ученых признает электронные носители информации отдельным видом доказательств.

Обосновывая свою позицию, представители первой группы ученых обращаются к толкованию положений ст. 84 УПК РФ: «документы, содержащие информацию об обстоятельствах, подлежащих доказыванию, могут фиксировать эту информацию в письменном и ином виде. К иным доку-

[1] Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2019. № 4. С. 48.

ментам могут относиться и иные носители информации, полученные, истребованные или представленные в порядке, установленном ст. 86 УПК РФ». Е. К. Губарев отмечает: «под иными носителями информации, указанными в ч. 2 ст. 84 УПК РФ, законодатель понимает именно электронные носители информации»[1].

Чтобы установить возможность отнесения электронных носителей информации к «иным документам» как источнику доказательств, следует определиться с понятием «документированная информация».

Так, согласно ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» «под документированной информацией следует понимать зафиксированную на материальном носителе путем документирования информацию с реквизитами, позволяющими определить такую информацию или ее материальный носитель»[2]. Рассматриваемый термин «связан» с поиском, получением, передачей информации, которые осуществляются с применением информационных технологий и требуют соответствующей защиты информации[3]. Сказанное применимо к понятию «иной документ» в уголовном судопроизводстве, т. к. в процессе любого расследования осуществляются поиск, получение и защита информации.

По мнению А. В. Ткачева, «отличить документ от недокументированной информации и отнести электронный документ на материальном носителе к иным документам позволяет наличие специальных реквизитов»[4]. В данном случае, конечно, больше вопросов, чем ответов, особенно если речь идет о преобразовании информации из электронного/виртуального вида на материальный носитель; кроме этого, если электронный носитель фактически не изымался, а была изъята информация в виде копирования файла, также не совсем ясно, каким же доказательством будет являться данная информация.

---

[1] Губарев Е. К. Информация, содержащаяся на электронном носителе, как вид доказательства по уголовному делу // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов : сборник международной научно-практической конференции. Самара, 2019.С. 151.

[2] Об информации, информационных технологиях и о защите информации : федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Российская газета. 2006. № 165.

[3] Маркелов А. Г. Иные документы как доказательства в российском уголовном процессе : дис. … канд. юрид. наук. Н. Новгород, 2019. С. 48.

[4] Ткачев А. В. Вопросы использования электронных носителей компьютерной информации в уголовном процессе в качестве доказательств иных документов // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 3. С. 438.

Процессуалисты, относящие электронные носители информации к вещественным доказательствам, в том числе А. А. Орлова[1], И. С. Федотов, П. Г. Смагин[2], ссылаются на следующие положения УПК РФ:

– ч. 4 ст. 81 УПК РФ, которая включает в предметы, не признанные вещественными доказательствами и подлежащие возврату, электронные носители информации;

– п. 5 ч. 2 ст. 82 УПК РФ[3] – устанавливает порядок хранения вещественных доказательств в виде электронных носителей информации;

– ч. 1 ст. 81.1 УПК РФ, которая гласит, что «при расследовании преступлений в сфере экономики, электронные носители информации признаются вещественными доказательствами и приобщаются к материалам уголовного дела, о чем выносится соответствующее постановление».

По мнению Л. Б. Красновой, «электронные носители информации должны иметь статус вещественного доказательства, т. к. они обладают присущими им признаками: в некоторых случаях становятся средством установления обстоятельств уголовного дела и содержат не только информацию о факте преступления, но и его следы; информация хранится на материальных носителях, а не в вербальной форме; получать, хранить и передавать невербальную информацию с них можно материальным способом»[4].

Так, согласно обвинительному заключению Н. своими умышленными действиями совершил мошенничество с использованием электронных средств платежа с причинением значительного ущерба гражданину, то есть преступление, предусмотренное ч. 2 ст. 159.3 Уголовного кодекса Российской Федерации[5] (далее – УК РФ).

Доказательствами, подтверждающими обвинение Н. в совершении преступления, предусмотренного ч. 2 ст. 159.3 УК РФ, являются:

– постановление о признании и приобщении к уголовному делу вещественных доказательств, согласно которому в качестве вещественных

---

[1] Орлова А. А. Место электронных носителей информации в системе доказательств по уголовным делам // Молодой ученый. 2019. № 15. С. 288.

[2] Федотов И. С., Смагин П. Г. Электронные носители информации: «вещественные доказательства» или «иные документы»? // Вестник Воронежского государственного университета. Серия: Право. 2020. № 3. С. 196.

[3] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : федеральный закон Российской Федерации от 28 июля 2012 г. № 143-ФЗ // Собрание законодательства Российской Федерации. 2012. № 31. Ст. 4332.

[4] Краснова Л. Б. Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 4. С. 258.

[5] Уголовный кодекс Российской Федерации от 24 мая 1996 г. Доступ из справ.-правовой системы «КонсультантПлюс».

доказательств признаны: банковская карта ПАО «СбербанкMOMENTUM R», имеющая номер 4817 7601 3462 7656; шесть фрагментов видеозаписей с камер видеонаблюдения из магазина «Маяк»; сведения о движении денежных средств ПАО «Сбербанк России» – отчет по счету банковской карты Ш. (т. 1, л. д. 79–80);

– протокол осмотра предметов и документов, согласно которому были осмотрены: отчеты по счету банковской карты ПАО «Сбербанк России» VISA MOMENTUM, имеющей номер 4817 7601 3462 7656, выданной на имя Ш. (т. 1, л. д. 125–128);

– постановление о признании и приобщении к уголовному делу вещественных доказательств, согласно которому в качестве вещественных доказательств признаны: отчеты по счету банковской карты ПАО «Сбербанк России» VISA MOMENTUM, имеющей номер 4817 7601 3462 7656, выданной на имя Ш. (т. 1, л. д. 130–132).

Третья группа ученых-процессуалистов признает данные с электронных носителей информации отдельным видом доказательств. К примеру, Ю. М. Батурин обосновывает свою позицию следующим образом: «записи в памяти электронных вычислительных машин преобразуется в код и потому оценке подлежит не только они [записи], но и программа съема информации, а также их совокупность»[1].

Н. А. Зигура выделяет компьютерную информацию как самостоятельный вид доказательств, т. к. «фиксация информации при помощи электронно-вычислительной машины происходит без ее переработки сознанием человека, в той форме, в какой она объективно существовала независимо от субъективного восприятия того, кто ее закрепляет, что свидетельствует о большой ценности данной информации и необходимости более эффективного использования ее в доказывании»[2].

В. Н. Григорьев, О. А. Максимов призывают «выделить электронные носители информации в отдельный источник доказательств, т. к. они содержат значимую информацию, восприятие которой невозможно без использования электронно-вычислительных средств. Такой подход позволит относить к указанному источнику доказательств любое оборудование, используемое в современном информационном процессе и содержащее незаменимую информацию, имеющую значение для дела»[3].

---

[1] Батурин Ю. М. Компьютерная преступность и компьютерная безопасность : учебное пособие. М. : Юридическая литература, 2020. С. 37.

[2] Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательств в уголовном процессе России : монография. М. : Юрлитинформ, 2020. С. 28.

[3] Григорьев В. Н., Максимов О. А. Некоторые вопросы использования электронных носителей информации при расследовании уголовных дел // Полицейская деятельность. 2018. № 1. С. 18.

Судебная практика по данному вопросу также неоднозначна. Суды в зависимости от роли информации в совершенном преступном деянии относят электронные носители информации как к иным документам, так и к вещественным доказательствам.

На практике суды чаще признают электронные носители информации вещественными доказательствами[1], т. к. они являются средствами или орудиями преступлений. Так, суд, вынося приговор по уголовному делу, отметил следующее: «телефоны и содержащаяся в них любая информация, в том числе видеозаписи и фотографии, не являются электронными носителями информации, а представляют собой предметы бытового повседневного пользования, которые содержат в себе определенную информацию, для получения которой специальных познаний не требуется»[2]. Практика свидетельствует и о том, что некоторые суды относят электронные носители информации к категории иных документов[3].

В связи с тем, что рассматриваемый вопрос однозначно не решен ни на законодательном уровне, ни в практике судов, ни в доктрине, к какому источнику доказательств относить электронные носители информации, решает сам правоприменитель. Для этого он оценивает содержащуюся на носителе доказательственную информацию, определяет ее значение для расследования преступления.

В заключение отметим существование еще одного дискуссионного вопроса в науке уголовного процесса – необходимости закрепления обобщенного понятия «электронное доказательство» в УПК РФ. Мнения ученых-процессуалистов на этот счет разделились. Одни отстаивают крайнюю необходимость закрепления указанного понятия, «без которого в теории и на практике возникает множество споров»[4], другие доказывают необязательность такого закрепления. Причем первая группа ученых обосновывает свою позицию новизной электронного доказательства как отдельного вида, а вторая отмечает, что «при использовании электронных доказа-

---

[1] Дело № 1-657/2020. Приговор суда Железнодорожного района г. Ростова-на-Дону от 12 ноября 2020 г. // Архив суда Железнодорожного района г. Ростова-на-Дону.

[2] Дело № 1-25/18. Приговор Ленинского районного суда г. Ульяновска от 19 мая 2018 г. // Архив Ленинского районного суда г. Ульяновска.

[3] Определение Конституционного Суда Российской Федерации от 11 мая 2012 г. № 814-О // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024); Апелляционное определение Верховного Суда Российской Федерации от 4 июня 2013 г. № 41-АПУ13-13сп // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024).

[4] Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательств в уголовном процессе России : монография. М. : Юрлитинформ, 2020. С. 33.

тельств не происходит переворота в процедуре и способе доказывания»[1]. Считаем возможным согласиться с последней позицией, т. к. информация, представленная в электронном виде, используемая в доказывании (электронные доказательства), не вносит ничего нового в закрепленную систему доказательств. Такого рода доказательства подлежат оценке правоприменителем по внутреннему убеждению так же, как и все остальные виды доказательств, т. е. форма их представления не влияет на «традиционные» принципы собирания, исследования и оценки уголовно-процессуальных доказательств.

На основе проведенного в параграфе исследования считаем возможным заключить следующее. В связи с тем, что закон не дает определения понятия «электронный носитель информации», а научные подходы очень разнообразны, существует острая необходимость его законодательного закрепления, что облегчит практическое применение рассматриваемого вида доказательств. Определение должно исключать его произвольную интерпретацию и подмену на практике, в связи с чем необходимо дать не техническое описание понятия, а указать его значение как источника доказательств.

Электронные носители информации как источники доказательств в зависимости от конкретной ситуации могут быть выступать вещественными доказательствами или иными документами. При этом определения понятий «вещественное доказательство» и «иные документы» целесообразно дополнить уточнением, что такие сведения могут быть представлены в виде электронной информации.

Если электронный носитель информации был орудием (средством) преступления, был получен в результате преступления, выступил в качестве средства обнаружения преступления и установления обстоятельств уголовного дела, был объектом посягательства, он может быть признан вещественным доказательством. Когда же на первый план выходит информационное содержание, а не физические характеристики электронного носителя, позволяющее установить обстоятельства, подлежащие доказыванию, он признается иным документом.

§ 2. Правовой режим доказательственной информации, представленной в электронном виде

Деятельность по формированию доказательств в виде информации, представленной в электронном виде, находится в прямой зависимости от правового режима последней. Ее правовой режим отражает установленные

[1] Пастухов П. С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества : монография / под ред. О. А. Зайцева. М. : Юрлитинформ, 2019. С. 72.

для такого рода информации ограничения, а также специальные юридические процедуры, которые в обязательном порядке следует соблюдать при формировании доказательств на ее основе.

Для уяснения особенностей правовых режимов доказательственной информации, представленной в электронном виде, необходимо проанализировать имеющиеся основания для ее классификации и, соответственно, виды такой информации.

1. По форме представления:

– документированная информация – данные, зафиксированные на материальном носителе с целью сохранности, и имеющие реквизиты: реквизиты позволяют установить характер самих данных и материального носителя (информационная функция), а также защищают данные (документы) от фальсификации (защитно-удостоверительная функция); к документированной информации относятся законодательные акты (нормативно-правовая база), документы библиотечных и других фондов, архивы, сведения средств массовой и публичной информации);

– недокументированная информация – данные, которые не обладают признаками документа и не имеют соответствующих реквизитов (логин и пароль пользователя в сети Интернет, ключи электронной цифровой подписи и т. п.).

Приведенная классификация позволяет отнести информацию, представленную в электронном виде, к тому или иному виду доказательств: к иным документам (когда для доказывания важно именно содержание документированной информации), вещественным доказательствам (если речь идет о недокументированной информации либо о документированной информации, которая несет на себе следы преступления)[1].

2. По критерию доступности информации, представленной в электронном виде:

– общедоступная информация – это «общеизвестные сведения и иная информация, доступ к которой не ограничен»[2]; такая информация обычно содержится в информационных системах, доступ к которым ни для кого неограничен, и получить ее может любой пользователь без специальных разрешений от собственника, иного лица (новости, сервисы объявлений, информация, размещаемая государственными органами и органами местного самоуправления в сети Интернет в форме открытых данных и т. д.);

– необщедоступная информация – это информация с ограниченным доступом, которая недоступна для третьих лиц, не обладающих законным

---

[1] Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. … канд. юрид. наук. М., 2020. С. 53.

[2] Об информации, информационных технологиях и о защите информации : федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Российская газета. 2006. № 165.

или специально полученным правом доступа к ней. Ограничение на доступ к той или иной информации устанавливает ее собственник (правообладатель) или закон.

Особый вид необщедоступной информации представляет тайна, которая охраняется законом, имеет специальный юридический механизм защиты, который может быть «преодолен» в необходимых случаях (в том числе для целей уголовного судопроизводства). К таким видам тайн относятся: государственная, коммерческая, банковская, иные профессиональные тайны (врачебная, нотариальная, адвокатская, журналистская, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений, тайна следствия, тайна голосования и т. д.)[1]. Представленный перечень тайн, не являющийся исчерпывающим, демонстрирует, насколько много видов информации, изъятие и использование которой в рамках уголовного судопроизводства имеет особенности, ограничения. Отметим, что наиболее часто в процессе доказывания по уголовным делам используется информация, относящаяся к коммерческой тайне (50 %), банковской тайне (35 %), тайне переписки, телеграфных сообщений, телефонных переговоров (15 %)[2].

3. Исходя из связи информации, представленной в электронном виде, с событием преступления (характер связи влияет на процессуальную форму собирания доказательственной информации, находящейся на электронных носителях):

– информация, которая служила орудием совершения преступления (вредоносные программы, программные приложения с алгоритмом действий, направленные на преступные действия, программы по подбору паролей);

– информация, которая сохранила на себе следы преступления (модификация, преобразование компьютерной информации, т. е. любые ее изменения);

– информация, на которую были направлены преступные действия (охраняемая законом компьютерная информация, которая находится на электронном носителе, в системе или их сети);

– иная компьютерная информация, которая устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела[3].

---

[1] Першин А. Н. Электронный носитель информации как новый источник доказательств по уголовным делам // Уголовный процесс. 2019. № 5. С. 52.

[2] Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. … канд. юрид. наук. М., 2020. С. 54.

[3] Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательств в уголовном процессе России : монография. М. : Юрлитинформ, 2020. С. 55.

По мнению автора данной классификации, она позволяет установить обстоятельства, входящие в предмет доказывания, и, соответственно, достичь цели уголовно-процессуального доказывания в целом.

4. По отношению к предмету доказывания информация, представленная в электронном виде, включает в себя фактические данные (информация о юридически значимых фактах и обстоятельствах, имеющих значение для дела) и метаданные (информация о признаках фактических данных, характеризующих обстоятельства их создания и модификации)[1].

Ю. В. Гаврилин выделяет такой вид информации, как электронный документ – «документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»[2].

А. П. Вершинин считает, что «существенными признаками электронного документа являются его содержание (информация) и форма (технический электронный носитель информации). Электронным документом является информация, зафиксированная на электронных носителях и содержащая реквизиты, позволяющие ее идентифицировать»[3].

По мнению О. А. Городова, признаками электронного документа являются:

– наличие материального носителя информации;

– наличие реквизитов, с помощью которых идентифицируются содержащиеся на материальном носителе сведения, устанавливается источник их происхождения, время документирования, а также обеспечивается защита документа от подделки;

– возможность изменения формы фиксации документированной информации, т. е. информация, зафиксированная на материальном носителе одного вида, может быть одновременно представлена и на других видах носителей без угрозы утраты своего содержания и реквизитов.

О. А. Городов отдельно рассматривает такие понятия, как:

– электронное сообщение как информацию, переданную или полученную пользователем информационно-телекоммуникационной сети;

– сайт в сети Интернет;

– страница сайта в сети Интернет;

– доменное имя;

---

[1] Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. … канд. юрид. наук. М., 2020. С. 56.

[2] Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2019. № 4 (44). С. 48.

[3] Вершинин А. П. Электронный документ: правовая форма и доказательство в суде. М., 2020. С. 41.

– системная информация;

– индивидуализирующая пользователя информация (пароли, коды доступа, электронная подпись, др.);

– база данных[1].

На основании вышеизложенного считаем возможным заключить следующее. Форма и вид информации, содержащейся на электронном носителе, достаточно разнообразны, – это может быть ориентирующая криминалистически важная информация, определяющая алгоритм следственных действий. Процессуальный порядок собирания доказательственной информации, представленной в электронном виде, напрямую зависит от вида и особенностей самой информации, что наглядно продемонстрировали приведенные выше классификации: по возможности доступа к информации третьих лиц; по юридическому механизму правовой защиты информации; по отношению к предмету доказывания; с учетом связи информации с событием преступления.

§ 3. Законодательные и правоприменительные аспекты получения сведений приватного характера при формировании предмета доказывания по преступлениям, совершенным с использованием современных цифровых и компьютерных технологий

Условия современного российского социума предоставили нам богатый спектр способов и возможностей не только активно пользоваться в своей повседневной жизни громадным объемом информации, но и делиться полученными данными с другими субъектами-пользователями. Со временем подобный обмен информацией превратился в неуправляемый процесс, потребовавший от законодателя экстренного вмешательства с целью законодательной регламентации на государственном уровне проблемы несанкционированного доступа к информационным сведениям, содержащимся в различных источниках, в том числе и на цифровых носителях, чтобы тем самым хотя бы минимизировать, а в идеале ликвидировать подобные случаи.

Законодатель не всегда своевременно реагирует на вышеуказанный процесс, так как процесс принятия нормативных правовых актов в качестве оградительных мер имеет длительный период. Приоритетной задачей для законодателя и правоприменителя выступает прежде всего качественная защита граждан от осуществляемого без разрешения собственника и пользователя доступа к конфиденциальной информации.

---

[1] Городов О. А. Основы информационного права России. СПб. : Юридический центр Пресс, 2019. С. 45.

Стоит подчеркнуть, что эти меры принимались еще в начале 90-х годов прошлого столетия, в экстренном порядке, в эпоху становления молодого российского государства. И по вполне понятным причинам принятая «в непростые времена» законодательная база подвергалась последующим дополнениям и изменениям.

В первую очередь положения, ограждающие приватную жизнь добросовестных и законопослушных граждан, зафиксированы в главном законе страны – Конституции Российской Федерации, в частности, в ст. 23, гарантирующей каждому защищенность его личного пространства, частной жизни, личной и семейной тайны, а также предоставляющей ему правовую защиту его доброго имени и чести[1]. За малейшее отступление от требований вышеуказанных конституционных предписаний предусмотрено наступление уголовной ответственности за посягательство на приватную жизнь по ч. 1 ст. 137 УК РФ за незаконные сбор и распространение информации из личной, частной жизни человека, сведений, составляющих семейную тайну, без получения его разрешения на такое распространение.

Несанкционированный сбор информации из личной, семейной, частной жизни означает умышленные и несанкционированные действия, направленные на получение информации любыми путями: через личное наблюдение, прослушивание, копирование документов, через аудио-, видео-, фотосъемку, а также посредством хищения или несанкционированного приобретения.

Положениями ст. 24 Конституции Российской Федерации наложен запрет на несанкционированные собирание, хранение, распространение и использование сведений из семейной, личной жизни человека. В целях борьбы с несанкционированным доступом к частной жизни граждан законодателем был вполне своевременно введен в действие Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», который ограждает всех законопослушных граждан от незаконного аккумулирования их персональной информации, доступ к которой разрешен только в исключительных случаях и с соблюдением требований конфиденциальности при работе с персональными данными госорганам, должностным или иным третьим лицам[2].

Законы, действующие на территории российских субъектов, ограждают от несанкционированного доступа к ним следующие виды данных и информации: а) сведения, имеющие отношение к государственной

---

[1] Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Собрание законодательства Российской Федерации. 2014. № 31. Ст. 4398.

[2] О персональных данных : федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

тайне[1]; б) сведения, затрагивающие частную или семейную жизнь гражданина, его личные, персональные сведения, относящиеся к категории конфиденциальных сведений[2].

Достаточно эффективным заградительным действием в защите частной, семейной и личной сфер жизнедеятельности гражданина от вторжения извне, помимо его воли, обладает Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а именно ч. 8 ст. 9 данного закона, которая запрещает истребовать от гражданина сведения из его частной и семейной жизни вопреки его воле, кроме тех ситуаций, когда это предусмотрено федеральным законодательством.

Стоит отметить, что у правоохранительных и судебных органов имеются вполне легальные «инструменты» для существенного сужения и даже ограничения неприкосновенности частного пространства гражданина, позволяющие им без получения на то разрешения от субъекта проникать в частную жизнь.

Одним из таких инструментов как раз и выступает УПК РФ. Увы, в действующем варианте УПК РФ до сих пор отсутствует детальная регламентация общих требований-условий единого механизма предоставления подобной информации. Как известно, тайна частной жизни гражданина может быть нарушена компетентными органами в связи со следственными действиями и мероприятиями по проникновению в жилище, по ограничению тайны телефонных и иных переговоров, переписки.

Правоохранительные органы и судебные инстанции могут располагать информацией из приватной жизни гражданина либо по результатам проводимых ими следственных действий, либо со слов иных участников судопроизводства, либо через исполненные запросы в органы государственной власти, учреждений и организаций.

Федеральный закон от 4 марта 2013 г. № 23-ФЗ «О внесении изменений в статью 62 и статью 303 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» наделил органы предварительного следствия правом собирать информацию из частной жизни граждан в целях сбора доказательственной базы до этапа возбуждения уголовного дела еще на стадии проверки сообщений о преступ-

---

[1] О государственной тайне : федеральный закон Российской Федерации от 21 июля 1993 г. № 5485-1. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об информации, информационных технологиях и о защите информации : федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3448.

лении[1]. Следует отметить и оборотную сторону подобной доследственной проверки, которая в данном контексте становится тождественной процессу расследования уголовного дела, а это означает, что у гражданина уменьшается арсенал средств правовой защиты своей частной жизни.

Обыск и выемка в жилище (ст. 182, 183 УПК РФ), наложение ареста на почтово-телеграфные отправления (ст. 185 УПК РФ), контроль и запись переговоров (ст. 186 УПК РФ), получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ) могут быть произведены только после возбуждения уголовного дела, так как информация и сведения, полученные в ходе вышеуказанных следственных мероприятий, относятся к категории «приватного» характера, а потому сбор подобной информации возможен только по судебному решению.

Наряду с этим законодателем допускается возможность получения информации приватного характера при применении других способов, таких как: допрос, наложение ареста на имущество, банковские счета и т. д. Ключевым во всех вышеперечисленных следственных действиях является тот факт, что они позволяют следственным и судебным органам получить законным способом максимальный объем информации о частной стороне жизни граждан и обеспечивают, таким образом, доступ к «тайнам приватной жизни».

Положения существующего УПК РФ, к сожалению, не содержат исчерпывающий список поводов-оснований производства следственных действий, ограничивающих право человека на тайну личной жизни. Существуют профессии, представители которых по роду своей профессиональной деятельности вынуждены сталкиваться и обращаться со сведениями из категории приватного характера своих «клиентов-доверителей»: работник органов записи актов гражданского состояния (далее – ЗАГСа), врач, нотариус, которые обязаны в силу своего должностного функционала хранить профессиональную тайну. Уголовно-процессуальное законодательство лишь регулирует порядок получения информации, в том числе доверенной гражданам или должностным лицам и касающейся информации частного характера конкретного физического лица. Отказавшись от дачи показаний, свидетель из списка вышеназванных должностных лиц может быть подвергнут уголовному преследованию по ст. 308 УК РФ. Исключением из этого списка выступает профессия священнослужителя, который обладает своего рода свидетельским иммунитетом, запрещающим его допрашивать

[1] О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : федеральный закон Российской Федерации от 4 марта 2013 г. № 23-ФЗ // Собрание законодательства Российской Федерации. 2013. № 9. Ст. 875.

в качестве свидетеля по поводу сведений, о которых он узнал из проведенной между ним и его прихожанином исповеди. Данное правило о так называемой тайне исповеди находит свое выражение в двух различных нормативных правовых актах: п. 4 ч. 3 ст. 56 УПК РФ и новеллах Федерального закона от 26 сентября 1997 г. № 3-ФЗ «О свободе совести и религиозных объединениях»[1].

В различных отраслях права существует также и ряд норм, которые не только предписывают правила предоставления частной информации правоохранительным и судебным органам, но и ориентированы прежде всего на защиту частной тайны гражданина, доверенной представителю определенной профессии. К таковым следует отнести п. 7 ч. 5 ст. 19 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», который предоставляет пациенту право на защиту врачебной тайны[2]. Только на основании официального письменного запроса компетентных органов в связи с проведением расследования или судебным разбирательством врачи или медицинские работники предоставляют информацию частного характера без какого-либо письменного согласия гражданина. Этот же закон обязывает медицинских работников сообщать информацию немедленно, без каких-либо запросов, в правоохранительные органы в целях информирования последних о поступлении какого-либо пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате криминального деяния.

Далее целесообразно упомянуть еще об одной специфической профессии, такой как нотариус, и его нотариальной тайне, а также о тайне записи актов гражданского состояния. Нотариальная тайна и тайна регистрации свидетельств гражданского состояния законодателем защищены от несанкционированного доступа и относятся к категории конфиденциальной информации с ограниченным доступом.

Согласно ч. 3 ст. 12 Федерального закона от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния», сведения, ставшие известными сотруднику органа ЗАГСа в связи с государственной регистрацией акта гражданского состояния, являются персональными данными, относятся к категории закрытой информации с ограниченным доступом и не подлежат распространению в открытых источниках. Одновременно с этим по

---

[1] О свободе совести и религиозных объединениях : федеральный закон Российской Федерации от 26 сентября 1997 г. № 3-ФЗ // Собрание законодательства Российской Федерации. 2002. № 23. Ст. 2102.

[2] Об основах охраны здоровья граждан в Российской Федерации : федеральный закон Российской Федерации от 21 ноября 2011 г. № 323-ФЗ // Собрание законодательства Российской Федерации. 2011. № 48. Ст. 6724.

официальному запросу компетентных органов руководитель органа ЗАГСа обязан предоставить информацию о государственной регистрации брака[1].

Что касается нотариальной тайны, несмотря на то, что на нотариуса при исполнении служебных обязанностей, а также на сотрудников нотариальной конторы распространяется запрет разглашать сведения, предавать огласке содержание документов, ставшие им известными ввиду совершения нотариальных действий, в том числе и после сложения полномочий или увольнения, одновременно с этим положением закон допускает «вторжение в конфиденциальность» нотариальной деятельности, когда в связи с расследованием уголовного дела нотариусы обязаны предоставлять компетентным органам в виде справочной информации сведения о совершении гражданами каких-либо юридических сделок[2].

Параллельно с изменениями, происходившими в уголовно-процессуальном законодательстве, и гражданско-правовая нормативная база претерпела за последнее время существенные изменения и поправки: к примеру, ст. 152.2 Гражданского кодекса Российской Федерации (далее – ГК РФ), согласно новой редакции, запрещает не только сбор, хранение, распространение, но и какое-либо несанкционированное использование сведений частного характера при отсутствии согласия самого субъекта[3].

Конституционный принцип неприкосновенности частной жизни, будучи закрепленным еще в 1993 году в тексте Конституции Российской Федерации, в некоторой степени продублирован в текстах многих нормативных правовых актов середины 90-х годов. Например, текст Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» повторяет конституционное требование о соблюдении неприкосновенности сведений частного характера при проведении оперативно-розыскных мероприятий[4]. Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне» требует того же от компетентных органов при проведении каких-либо проверочных мероприятий в период оформления допуска к сведениям, составляющим государственную тайну[5], и многое др.

---

[1] Об актах гражданского состояния : федеральный закон Российской Федерации от 15 ноября 1997 г. № 143-ФЗ // Собрание законодательства Российской Федерации. 1997. № 47. Ст. 5340.

[2] Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-I // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1993. № 10. Ст. 357.

[3] Гражданский кодекс Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. (ч. I). Ст. 3301.

[4] Об оперативно-розыскной деятельности : федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

[5] О государственной тайне : федеральный закон Российской Федерации от 21 июля 1993 г. № 5485-1. Доступ из справ.-правовой системы «КонсультантПлюс».

Несмотря на быстрое развитие компьютерных технологий, проблемы защиты частной жизни и статуса информации о гражданине стали подпадать под «зоркое око» законодателя только лишь с середины нулевых годов. Одновременно, в один и тот же день, а именно 27 июля 2006 года, законодатель принял Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1] и Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[2]. В первом случае законодатель закрепил в качестве одного из принципов неприкосновенность частной жизни. Во втором же случае – наложил запретна обработку личных данных без разрешения гражданина.

Анализируя далее законодательство в хронологической последовательности, целесообразно отметить, что помимо ст. 152.2 ГК РФ 1 октября 2013 года ст. 152 ГК РФ пополнилась п. 10, позволившим гражданам и организациям рассчитывать на компенсацию вреда, причиненного не только распространением порочащих честь, достоинство и доброе имя сведений, но и заведомо ложной информации[3].

Проведя сравнительную параллель с зарубежными, в частности, с западно-европейскими державами (Германией, Францией, Австрией), нам, как правоприменителю, «бросается в глаза» относительно недавний срок функционирования и введения в действие в отечественном законодательстве закрепленной в ст. 152.2 ГК РФ нормы, касающейся охраны частной жизни гражданина. Как видно, приоритет российский законодатель отдал понятию «тайна частной жизни», под которым понимается вся совокупность приватной информации из личной жизни человека.

Более детализированному толкованию термин «частная жизнь» подвергнут в Определении Конституционного Суда Российской Федерации от 9 июня 2005 г. № 248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации», согласно которому право на неприкосновенность частных сведений предполагает возможность гражданина контролировать информацию о себе и препятствовать распространению сведений интимного характера. Иными словами, если приватная сторона жизни человека не носит противозаконный характер, то она и не подлежит контро-

---

[1] Об информации, информационных технологиях и о защите информации : федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Рос. Федерации. 2006. № 31 (ч. 1). Ст. 3448.

[2] О персональных данных : федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Гражданский кодекс Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32 (ч. I). Ст. 3301.

лю со стороны общества и государства. Стоит отметить, что, к сожалению, и эта дефиниция не может дать развернутый ответ на вопрос относительно того, кто именно определяет границы частной жизни гражданина: сам субъект-индивид или подобные границы должны быть кем-то объективно очерчены?

В том случае, когда гражданин выступает субъектом правоотношений, нормы ст. 152.2 ГК РФ предоставляют ему обширные возможности, что способствует порождению противоречивой судебной практики. Конституционный Суд Российской Федерации рассматривает частную жизнь именно в таком контексте, поэтому в одном из своих определений, связанных с отказом в принятии к рассмотрению жалобы на нарушение конституционных прав ст. 137 УК РФ, вынесенных еще в июне 2012 года, было указано, что «только сам человек вправе определить для себя и окружающих, какая информация личного характера и в каком именно объеме не подлежит разглашению, а остается тайной».

Даже из правила запрета на сбор, хранение, распространение и использование любой информации о частной жизни гражданина есть некоторые изъятия. К примеру, п. 2 ст. 152.2 ГК РФ не считает такие действия запрещенными, если они осуществляются в интересах государства, общества. По сути, это означает, что государственные и муниципальные органы и учреждения вправе подвергать обработке информацию о гражданах в своей профессиональной деятельности.

Однако в наш «век больших цифровых технологий» часто происходит «утечка» информации, и та сторона частной жизни, охране которой служит вышеупомянутые нормативные акты, с легкостью может быть «взломана» действиями так называемых хакеров. В этом случае объектом преступного посягательства становится один из видов информации – компьютерная информация, или информация, содержащаяся на цифровых носителях.

В связи с участившимися случаями подобных взломов ученые-криминалисты и ученые-процессуалисты были единогласны в своем мнении о возникшей целесообразности правового закрепления на законодательном уровне термина «компьютерная информация». Вскоре ст. 272 пополнилась примечанием с подробным описанием данного термина. Ранее термин «компьютерная информация» трактовался как информация на машинном носителе или находящаяся в системе электронно-вычислительных машин (далее – ЭВМ) или их сети. Примечание к ст. 272 УК РФ же предлагает трактовать компьютерную информацию как «сведения, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[1].

[1] Уголовный кодекс Российской Федерации от 24 мая 1996 г. Доступ из справ.-правовой системы «КонсультантПлюс».

Чтобы разобраться, в каких случаях законодатель требует расценивать доступ к компьютерным сведениям в качестве неправомерного (несанкционированного), необходимо понимать, что в разряд неправомерного он переходит в том случае, когда такой доступ осуществляется в нарушение порядка, предписанного законодательной базой Российской Федерации, новелл, касающихся государственной тайны[1], персональных сведений[2], коммерческой тайны[3], банковской тайны[4], сведений по усыновлению ребенка[5] и многих др.

С принятием Указа Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»[6] существенно пополнился список сведений, обладающих признаком конфиденциальности, благодаря включению в него таких видов, которые содержат в себе: а) тайну следствия и судопроизводства; б) служебную тайну с ограниченном доступом пользования; в) врачебную, нотариальную, адвокатскую тайну, т. е. связанные с профессиональной деятельностью; г) коммерческую тайну, т. е. связанную с коммерческой деятельностью; д) тайну переписки, телефонных переговоров, почтовых и телеграфных сообщений-отправлений. К ним относятся также сведения б авторстве на изобретения о полезной модификации или промышленного образца, расцениваемые в качестве объектов смежных и авторских прав.

Действующее российское законодательство не требует корреляции компьютерной информации только лишь с ЭВМ-носителем. Предметом посягательства «киберзлоумышленников» при подобных преступлениях, совершенных с использованием высоких технологий, т. е. тем, что представляет криминалистическую ценность, выступают лишь те сведения и данные, которые еще не записаны на каком-либо устройстве (носителе), а находятся пока в процессе передачи.

---

[1] О государственной тайне : федеральный закон Российской Федерации от 21 июля 1993 г. № 5485-1. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О персональных данных : федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] О коммерческой тайне : федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] О банках и банковской деятельности : федеральный закон Российской Федерации от 2 декабря 1990 г. № 395-1 // Собрание законодательства Российской Федерации. 1996. № 6. Ст. 492.

[5] Постатейный комментарий к Семейному кодексу Российской Федерации, Федеральному закону «Об опеке и попечительстве» и Федеральному закону «Об актах гражданского состояния» / О. Г. Алексеева, В. В. Андропов, А. А. Бухарбаева [и др.]; под ред. П. В. Крашенинникова. М. : Статут, 2012. 656 с.

[6] Об утверждении Перечня сведений конфиденциального характера : указ Президента Российской Федерации от 6 марта 1997 г. № 188. Доступ из справ.-правовой системы «КонсультантПлюс».

Несмотря на то, что законодатель ввел в обиход такое определение, как электронный носитель информации, в уголовно-процессуальном законе до сих пор однозначно не указано, что именно следует понимать под термином «электронный (или цифровой) носитель информации».

Отечественная законодательная база, к сожалению, не содержит какого-либо четкого определения электронных или цифровых носителей информации, следов электронного присутствия, переработки информации. За неимением таковых за их толкованием приходится прибегать к нормативным правовым актам других отраслей законодательства. Обратимся к п. 3.28 ГОСТ Р 7.0.95-2015 «Система стандартов по информации, библиотечному и издательскому делу. Электронные документы. Основные виды, выходные сведения, технологические характеристики», где термин «электронный носитель информации» («электронный носитель данных») характеризуется как материальный объект, используемый для записи, хранения и воспроизведения цифровой информации[1].

Далее нам представляется целесообразным перечислить все многообразие электронных приспособлений, технических устройств, которые способны сохранить любую информацию, сведения или иные данные о подготовке, совершении или фактах сокрытия преступных посягательств, правонарушений и преступлений. К таковым относятся все современные телефоны, смартфоны, гаджеты, портативные устройства GPS (англ. Global Positioning System), цифровая фото- и видеоаппаратура, планшетники, видеорегистраторы, компьютеры, ноут- и нетбуки, навигаторы, платежные системы, диски, USB-устройства, карты памяти и т. д.

Вышеперечисленные устройства часто используются в качестве орудий совершения преступлений, а значит, могут содержать ценную информацию, представляющую интерес для органов предварительного следствия. Поэтому основной задачей органов предварительного следствия в борьбе с преступлениями, совершенными с использованием цифровых технологий, выступает получение вышеуказанной информации, хранящейся на цифровых носителях вышеперечисленных устройств, в установленном законом порядке.

В связи с этим справедливо возникает вопрос, кто обладает достаточным уровнем знаний, чтобы компетентно, на профессиональном уровне, без страха утраты следов преступления из-за низких познаний в области цифровых технологий, эффективно содействовать следственным органам

[1] ГОСТ Р 7.0.95-2015. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Электронные документы. Основные виды, выходные сведения, технологические характеристики (утв. И введен в действие приказом Росстандарта от 9 декабря 2015 г. № 2127-ст). М. : Стандартинформ, 2017.

в сборе доказательственной базы виновности киберпреступников, для ее качественного закрепления и последующей судебной перспективы, участвовать в изъятии мобильных средств связи, компьютеров, планшетов, процессоров, жестких дисков и иных цифровых носителей информации, содержащих в себе электронные следы взломов, с целью обеспечения не только сохранности имеющейся информации в цифровой памяти электронного носителя, но и всестороннего сопровождения уголовного дела, с привлечением к уголовной ответственности виновных «киберзлоумышленников».

В качестве таковых могут быть приглашены специалисты. Согласно уголовно-процессуальному законодательству, под специалистом следует понимать любое компетентное лицо, обладающее соответствующими познаниями в области цифровых, компьютерных устройств. В качестве специалистов можно привлекать консультантов специализированных отделов, компьютерщиков, программистов, которые в ходе проведения следственных действий содействуют следственным органам по изъятию и упаковке цифровых носителей информации, обеспечивают сохранность имеющейся информации в цифровой памяти электронного носителя. Приоритетной обязанностью лица, приглашенного в качестве специалиста при производстве следственного действия, выступает оказание содействия следственным органам в обнаружении, закреплении и (или) изъятии с электронных носителей важной для следствия информации, а также применение в этих целях технических приспособлений.

Из текста ч. 2 ст. 164.1 УПК РФ ясно видно, что электронные носители с имеющейся на них ценной информацией необходимо изымать в ходе следственного действия с участием специалиста[1]. Также во время копирования изымаемой информации для большей объективности производимого действия желательно пригласить двух понятых, с обязательным разъяснением всем участникам их прав и обязанностей.

С приходом в нашу жизнь процесса цифровизации, а затем переводом основных сфер жизнедеятельности современного человека из-за пандемии COVID-19 в дистанционный формат, произошел бурный прирост киберпреступности, увеличилась доля преступлений, совершенных с использованием информационно-телекоммуникационных и иных цифровых технологий. В связи с этим органы предварительного следствия стали чаще прибегать для сопровождения по уголовным делам компьютерщиков, IT-специалистов в качестве специалистов.

Законодательство позволяет привлекать в качестве таковых не только действующих экспертов, работающих в ведомственных учреждениях, в качестве действующих сотрудников, но и IT-специалистов из коммерче-

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Российская газета. 2001. № 249.

ских организаций, которыми могут выступать: системные и технические администраторы, консультанты различных специализированных фирм (или магазинов по продаже, ремонту цифровой и электронной техники), инженеры-программисты. К сожалению, такое многообразие специалистов «на рынке услуг» не всегда приносит положительный эффект и пользу для органов предварительного расследования и суда, ведь, как говорится, «специалист специалисту – рознь».

Несмотря на имеющуюся сформированную правоприменительную практику, очевидной «недоработкой» на законодательном уровне выступает наличие широкого выбора среди специалистов данного профиля, что вовсе не является стопроцентной гарантией наличия у последних достаточного уровня компетентности, практического опыта для успешного всестороннего, полноценного извлечения электронной информации и качественного, целостного изъятия цифровых накопителей, содержащих ценную для следствия информацию.

Каждый раз, обращая свой выбор на конкретного одного специалиста, следователь вынужден действовать под свою ответственность и работать «как бы на перспективу». Иными словами, следователь обязан заранее оценить и предусмотреть «на два шага вперед» перспективу признания судьей достаточной компетентности у отобранного следователем специалиста, так как от этого будут зависеть относимость и допустимость доказательства при принятии судом итогового решения по делу.

Мы полагаем, что в данном случае наличие выданной государственным органом специальной лицензии в области компьютерных и цифровых технологий облегчило бы следствию и суду возможности в выборе специалиста в этой области.

Резюмируя вышеизложенное, отметим, что возможность отступить от конституционных гарантий неприкосновенности тайны частной жизни граждан должна быть только у государственных органов правоохранительной системы и только в рамках уголовного дела, когда подобные сведения необходимы для реализации права потерпевших на защиту от преступных действий иных лиц, обеспечения всестороннего и полного уголовного расследования и последующего судебного производства.

ГЛАВА 2. ПРОБЛЕМЫ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИИ, ПРЕДСТАВЛЕННОЙ В ЭЛЕКТРОННОМ ВИДЕ, В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВА ПО УГОЛОВНОМУ ДЕЛУ

§ 1. Собирание доказательственной информации, представленной в электронном виде, в ходе следственных действий

Несмотря на дистанционный характер совершения преступлений с использованием информационных и телекоммуникационных технологий, им присуще следообразование, т. е. оставление на месте совершения преступления различных следов, дающих возможность с их помощью найти, идентифицировать преступника и пресечь его противоправную деятельность. Следы преступлений, совершенных с использованием телекоммуникационных технологий, криминалисты называют цифровыми или электронными.

Раскрываемость преступлений в сфере компьютерной информации находится на весьма низком уровне. Это обусловлено методами совершения преступления, позволяющими с большой вероятностью избежать разоблачения личности преступника и последующего наказания, такими как:

– использование услуг сотовых операторов связи с применением определенного сервера голосовой связи, способного защитить разговоры и сделать их доступными только для узкого круга лиц;

– шифрование данных на электронных носителях информации, позволяющее защитить конфиденциальную информацию от несанкционированного доступа, к примеру, прочтения или подмены;

– использование VPN (англ. virtual private network – «виртуальная частная сеть») в качестве сервиса, позволяющего скрыть и зашифровать личные данные при использовании сети Интернет, а также информацию о том, какие сайты были посещены в то или иное время;

– использование анонимайзеров для обеспечения конфиденциальности информации, а также посещения заблокированных сайтов на территории Российской Федерации.

Электронные следы можно классифицировать на две основные группы: статистические и динамические. При статическом следообразовании возникновение происходит посредством функционирования электронного устройства. К данному типу следов относятся, например, сведения об IP-адресе используемого устройства и его перемещения в телекоммуникационной сети Интернет.

Статистические электронные следы фиксируются провайдером интернет-услуг, непосредственно предоставляющим услуги пользования ресурсами связи, и в дальнейшем при соблюдении необходимых процессуальных требований могут быть переданы правоохранительным органам для производства расследования совершенного преступления.

К динамическому типу следообразования можно отнести электронные следы, формирующиеся в ходе операций человека или электронной системы, в результате чего появляется виртуальный объект, который в дальнейшем человек может использовать для различных целей. Ярким примером является комплекс операций по регистрации пользователя в сети Интернет.

Рассматривая электронные следы с позиции криминалистической классификации следов на идеальные и материальные, следует отметить, что единого мнения относительно принадлежности к той или иной группе нет. Некоторые ученые относят электронно-цифровые следы к материальным следам. При описании механизма следообразования по преступлениям, в результате совершения которых происходит изменение компьютерной информации, необходимо изучать электронно-цифровые следы как группу невидимых материальных следов.

Согласно мнению большинства криминалистов, доказательственная ценность компьютерных записей неоднородна и определяется целым рядом обстоятельств. К примеру, компьютерные файлы, содержащие текст, разделяются на несколько типов в зависимости от способа происхождения:

– файлы, созданные человеком и сохраненные на электронном носителе (например, постовые сообщения, служебные записи и т. п.);

– файлы, созданные компьютером в автоматическом режиме без участия человека (например, системные уведомления, записи в журнале системных событий, служебные сообщения о доставке электронной почты и т. п.);

– файлы, информация в которых скомпилирована компьютером с учетом последовательности операций, заданных человеком (например, файл, созданный программой финансового учета на основе исходных данных, введенных бухгалтером).

Таким образом, при совершении преступных деяний с использованием телекоммуникационной сети Интернет цель преступника – действовать инкогнито. Это определяет необходимость рассматривать виртуальные просторы сети Интернет как место совершения преступления, которое подлежит исследованию уголовно-процессуальными способами для сбора криминалистически важной информации. Указанные обстоятельства свидетельствуют о целесообразности более четкого правового урегулирования и выработки соответствующих методик расследования преступлений данной категории.

Органам предварительного расследования необходимо принимать меры для получения сведений о пользователях и их действиях на ресурсах сети Интернет в целях установления лица, совершившего преступление, и иных обстоятельств преступления.

Следует учитывать, что факты активности пользователя в сети Интернет (ведение переписки, публикация различной мультимедийной информации) не только отражаются на общедоступных ресурсах в виде текстовой визуальной информации, но и фиксируются организаторами распространения информации в сети Интернет на ее аппаратно-программных средствах (серверы, базы данных и т. п.) в виде определенных символов. Более того, согласно Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» организаторы распространения информации в сети Интернет обязаны хранить на территории Российской Федерации и предоставлять уполномоченным органам по запросу сведения, касающиеся:

– фактов приема, передачи, доставки и обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информации об этих пользователях (срок хранения таких сведений составляет один год с момента окончания осуществления этих действий);

– текстовых сообщений, голосовой информации, изображения, звуков, видео-, иных электронных сообщений пользователей сети Интернет (срок хранения таких сведений составляет до шести месяцев с момента окончания их приема, передачи, доставки и обработки).

Стоит отметить, что указанные сведения отражают информационную сторону взаимодействия пользователя сети Интернет с конкретным ее ресурсом. При этом нельзя забывать о технической стороне взаимодействия пользователя с сетью при подключении. В таком случае речь идет о данных устройства, с которого осуществлялся доступ в сеть Интернет, его IP-адресе соединения. Сведения о подключении пользователя к сети Интернет, отражающиеся на аппаратно-программных средствах связи сети Интернет в виде символов, необходимо получать в ходе следственного действия, регламентируемого ст. 186.1 УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». Требуется также разрешение суда о получении такой информации, которое направляется вместе с запросом в конкретную организацию (провайдеру, администратору интернет-ресурса). Важность получения указанной информации заключается в том, что она отражает как техническую сторону взаимодействия пользователя с сетью Интернет, так и информационную составляющую его действий на конкретном ресурсе.

Специфика и роль электронных носителей информации для расследования уголовных дел требуют гарантий сохранности в неизменном виде самого носителя при изъятии его в ходе следственных действий и исследовании в дальнейшем, а также достоверности содержащихся на нем сведений. УПК РФ закрепляет определенный порядок «работы» с указанными объектами.

Федеральным законом от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации»[1] в ст. 183 УПК РФ была введена ч. 3.1, которая установила особый порядок изъятия электронных носителей информации:

– выемку необходимо производить строго в присутствии специалиста;

– законному владельцу электронного носителя необходимо дать скопировать информацию с электронного носителя по его ходатайству.

Аналогичные законодательные положения были включены в ст. 182 УПК РФ, регулирующую производство обыска (ч. 9.1). Впоследствии Федеральным законом от 27 декабря 2018 г. № 533-ФЗ «О внесении изменений в статьи 176.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (далее – закон № 533-ФЗ) нормы ч. 9.1 ст. 182, ч. 3.1 ст. 183 УПК РФ были признаны утратившими силу. Взамен этим же законом была введена ст. 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий»[2].

Согласно ст. 164.1 УПК РФ «при производстве по уголовным делам, указанным в ч. 4.1 ст. 164 УПК РФ, изъятие электронных носителей информации не допускается, за исключением случаев, когда:

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

2) изъятие электронных носителей информации производится на основании судебного решения;

3) на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо она может быть использована для совершения новых преступлений, либо ее копирование, по заявлению специалиста, может повлечь за собой ее утрату или изменение»[3].

Новые нормы внесли существенные изменения в порядок изъятия электронных носителей и копирования с них информации по сравнению с отмененными положениями в этой области. Так, законодатель установил порядок изъятия электронных носителей и копирования информации, который распространяется на все следственные действия, а не только на обыск и выемку, как это было ранее. Также законом установлены огра-

---

[1] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : федеральный закон Российской Федерации от 28 июля 2012 г. № 143-ФЗ // Собрание законодательства Российской Федерации. 2012. № 31. Ст. 4332.

[2] О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : федеральный закон Российской Федерации от 27 декабря 2018 г. № 533-ФЗ // Российская газета. 2018. № 295.

[3] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Российская газета. 2001. № 249.

ничения, а именно запрет, на изъятие электронных носителей при производстве следственных действий по уголовным делам о преступлениях в сфере предпринимательской деятельности, за исключением случаев, указанных в ч. 1 ст. 164.1 УПК РФ.

Кроме того, обязательность привлечения специалиста при изъятии электронного носителя и копирования информации сохранена только для случаев изъятия непосредственно электронного носителя информации. Копирование информации с носителя следователь может провести самостоятельно, не изымая его. В таком случае привлечение специалиста выглядит как формальное исполнение нормы закона, и это влечет возникновение ряда вопросов, например, учитывая, что в правоохранительных органах нет штатных специалистов в сфере IT-технологий, возникает вопрос, каким образом обеспечить следственное действие специалистом, причем очень оперативно. С другой стороны, законодатель определяет обязательное участие специалиста, тем самым обеспечивая следователя оптимальным набором процессуальных средств для получения криминалистически важной информации, как бы предопределяя возникновение необходимости участия специалиста.

А. В. Ким считает, что «внесенные дополнения в УПК РФ направлены на защиту субъектов предпринимательства от необоснованного изъятия электронных носителей информации, которое может привести к приостановке хозяйственной деятельности»[1].

Таким образом, теперь согласно закону по многим преступлениям в сфере предпринимательской деятельности отсутствует возможность изъятия электронного носителя информации, по остальным же изымать можно, но с участием специалиста. Что делать следователю в случае невозможности изъятия электронного носителя информации – в законе не указано.

Далее отметим, что ограничивать конституционные права граждан в уголовном процессе возможно только на основании судебного решения (ст. 13 УПК РФ). Однако законом не предусмотрено получение решения суда для проведения осмотра изъятых в ходе расследования уголовного дела электронных носителей информации (к примеру, мобильных телефонов с содержащейся в них информацией). И это несмотря на то, что электронные носители могут и в большинстве своем содержат личную переписку, сведения частного характера, личную, семейную тайну. Такая ситуация влечет противоречивость практики по данному вопросу.

Так, согласно кассационному определению по делу № 22-2225/18 от 24 мая 2018 г. судебная коллегия по уголовным делам Омского областного суда отменила постановление Советского районного суда г. Омска от 16 апреля 2018 г. в части оставления без удовлетворения жа-

[1] Ким А. В. Отдельные вопросы проведения осмотра и экспертизы электронных носителей информации // Юридические науки. 2019. № 1. С. 153.

лобы адвоката на действия следователя по производству выемки мобильного телефона и осмотру сообщений в нем. В жалобе адвокат заявлял, что суд признал законным ограничение права потерпевшего на тайну переписки без судебного решения. Данное решение суда не основано на законе, т. к. осмотр телефона включает в себя осмотр телефонного аппарата, но не его содержимого. Судебная коллегия отметила, что в главе 25 УПК РФ прямо не закреплена обязанность следователя получать судебное решение на осмотр сообщений в мобильном телефоне, однако данная обязанность следует из других норм УПК РФ, положений Конституции Российской Федерации, а также из Конвенции о защите прав человека и основных свобод. Вывод о законности проведенного следственного действия, содержащийся в постановлении суда, основанный на том, что со стороны участников судопроизводства не поступило возражений на осмотр переписки, а телефон был выдан добровольно, представляется судебной коллегии неубедительным. В постановлении суд не учел, что переписка имеет двусторонний характер и включает в себя не только мысли потерпевшего, но и других лиц, не уведомленных о том, что их сообщения будут осматриваться. В кассационном определении указано, что при осмотре телефона следователем были довольно подробно описаны соединения между абонентами и суд в постановлении не учел, что ст. 186.1 УПК РФ устанавливает, что для получения информации о соединениях между абонентами необходимо судебное разрешение»[1]. Таким образом, в рассмотренном примере судебная коллегия допускает применение закона по аналогии.

Рассмотрим другой пример. В апелляционном определении Челябинского областного суда по делу № 10-2537/2018 от 30 мая 2018 г. апелляционная жалоба адвоката на приговор Увельского районного суда Челябинской области от 30 марта 2018 г. была оставлена без удовлетворения. В жалобе адвокат указал, что осматривать изъятые у осужденного предметы (телефоны) сотрудники без решения суда не имели права. Обсудив доводы апелляционной жалобы, изучив материалы уголовного дела, Челябинский областной суд приговор не отменил. Суд в апелляционном определении отметил, что УПК РФ не предусматривает необходимости вынесения судебного разрешения для проведения осмотра изъятых в ходе расследования уголовного дела мобильных телефонов, а доводы адвоката, который указывает на необходимость получения такого разрешения в соответствии с предписаниями ст. 186, 186.1 УПК РФ, ошибоч-

[1] Дело № 22-2225/18. Кассационное определение Омского областного суда от 24 мая 2018 г. // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024).

ны[1]. В рассматриваемом примере суд апелляционной инстанции не считает нарушением закона осмотр информации на телефоне, проведенный без судебного решения.

Также отметим, что по поводу осмотра электронных носителей, которые были изъяты в процессе производства следственного действия, проводимого на основании судебного решения, суды склоняются к возможности такого осмотра без решения суда. Например, Приморский краевой суд в своем апелляционном постановлении не усмотрел нарушений в постановлении Ленинского районного суда г. Владивостока от 27 ноября 2018 г., которым было отказано в удовлетворении ходатайства следователя о разрешении производства осмотра мобильных телефонов, изъятых в ходе производства обыска в жилище. Суд апелляционной инстанции указал, что телефоны, которые содержат переписку, были изъяты следователем в соответствии с процедурой, предусмотренной УПК РФ, в ходе обыска в жилище, который производился на основании решения суда и в целях изъятия электронных носителей информации и средств связи. Приморский краевой суд в апелляционном постановлении обратил внимание на то, что согласно УПК РФ не требуется судебное разрешение для производства осмотра протоколов телефонных соединений, предоставленных на основании судебного решения, а также что в соответствии со ст. 176, 177 УПК РФ изъятые в ходе обыска предметы при наличии времени и технической возможности могут быть осмотрены следователем на месте производства обыска[2].

Приведенные примеры судебной практики показали ее противоречивость, которая связана с неоднозначностью толкования норм УПК РФ. В своем определении от 25 января 20218 г. № 1890 «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Д. А. на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации» Конституционный Суд Российской Федерации разъяснил следующее: «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. Лица же, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну пере-

[1] Дело № 10-2537/18. Апелляционное определение Челябинского областного суда от 30 мая 2018 г. // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024).

[2] Дело № 22-455/19. Апелляционное постановление Приморского краевого суда от 2 февраля 2019 г. // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024).

писки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суд в порядке, предусмотренном статьей 125 УПК Российской Федерации»[1]. Конституционный Суд Российской Федерации по данной жалобе не вынес постановление о конституционности или неконституционности обжалуемых норм, указав на законность процессуальных действий и отсутствие необходимости получать соответствующее судебное решение. Таким образом, окончательной точки по этому вопросу Конституционный Суд Российской Федерации не поставил.

Анализ ст. 177, 182, 183, 184, 185, 186, 186.1 УПК РФ показывает, что для процессуальных действий, в которых предусмотрено ограничение конституционных прав граждан (неприкосновенность жилища, тайна переписки и частной жизни), продуман механизм разрешения данного следственного действия судом.

Так, например, отдельным следственным действием в ст. 186.1 УПК РФ оформлено получение информации о соединениях между абонентами и (или) абонентскими устройствами. Следователь не вправе запросить без разрешения суда данную информацию или произвести выемку вышеуказанных сведений у оператора связи. Однако ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[2] закрепляет обязанность операторов связи предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность, информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач. В данных случаях судебного решения не требуется. «Осмотр же почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда».

Если обыск и выемка электронного носителя информации производится в жилом помещении (здесь ограничение конституционных прав происходит, как известно, на основании судебного решения), то его осмотр осуществляется на основании этого же процессуального документа. Если указанные следственные действия производятся в нежилом помещении или в ходе осмотра места происшествия, то осмотр электронного носителя

---

[1] Об отказе в принятии к рассмотрению жалобы гражданина Д. А Прозоровского на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда Российской Федерации от 25 января 2018 г. № 189-О // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024).

[2] О связи : федеральный закон Российской Федерации от 7 июля 2003 г. № 126-ФЗ // Российская газета. 2003. 10 июля. № 135.

проводится без решения суда (соответствующего требования УПК РФ не содержит).

Как отмечает И. И. Карташов, «наибольшие проблемы вызывает вопрос о правовом статусе информации, которая содержится в мобильном телефоне, т. к. федеральное законодательство не содержит даже понятия электронной почты, не говоря уже о данных переписки из приложений для мобильных устройств»[1]. По мнению некоторых ученых, проблему можно решить введением в УПК РФ требования о необходимости получения разрешения суда для проведения осмотра или экспертизы электронного носителя, изъятого в ходе процессуальных действий, на которые санкция суда не требовалась.

Остановимся подробнее на тактике осмотра электронных носителей (и информации на них) и мест их обнаружения. С. В. Зуев отмечает, что «осмотр электронных носителей информации – это действие следователя в рамках осмотра места происшествия, а равно самостоятельное следственное действие по обнаружению, фиксации и изъятию преимущественно электронно-цифровых следов преступления и описанию признаков электронного носителя информации»[2].

Рассмотрим кратко деятельность следователя на подготовительном этапе осмотра места происшествия как способ получения доказательственной информации с электронных носителей. Цели проведения данного следственного действия применительно к рассматриваемым объектам не отличаются от типичных для осмотра места происшествия в целом:

1) получить исходные данные, которые позволят построить криминалистические версии, проверить уже имеющиеся;

2) получить новые и проверить имеющиеся доказательства.

Спецификой обладают задачи осмотра места происшествия как способа получения доказательственной информации с электронных носителей. Этими задачами являются следующие:

1) обнаружить, зафиксировать и изъять электронно-цифровые следы;

2) зафиксировать обстановку преступления, при совершении которого были оставлены электронно-цифровые следы, условия использования преступником электронных носителей информации[3].

Следователь обязан принять меры, которые не позволят уничтожить следы преступления, иным образом помешать осуществлению предварительного следствия. Для этого он (с помощью специалиста) должен:

---

[1] Карташов И. И., Лесников О. А. Цифровая информация в уголовно процессуальном доказывании: понятие и свойства // Наука. Общество. Государство. 2020. № 4 (32). С. 76.

[2] Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / отв. ред. С. В. Зуев. М. : Юрайт, 2020. С. 64.

[3] Савельева Н. В. Проблемы доказательств и доказывания в уголовном процессе : учебное пособие. Краснодар, 2019. С. 59.

1) установить тип программного обеспечения, характер взаимодействия компьютерных устройств, наличие подключения к сети;

2) выявить наличие средств защиты от несанкционированного доступа;

3) обеспечить сохранность обстановки на месте происшествия;

4) не допустить, чтобы компьютерная система преждевременно восстановилась[1].

Место проведения осмотра выбирается с учетом вероятного нахождения электронных носителей информации (главный компьютер локальной сети (сервер), персональные компьютеры, сейфы, и т. п.).

Время осмотра выбирается с учетом необходимости привлечения специалиста и других участников, присутствие которых необходимо; проведения осмотра как можно раньше, на первоначальном этапе расследования (этапе проверки сообщения о преступлении), чтобы информация на электронных носителях не была повреждена, уничтожена.

Специалист, привлекаемый к содействию:

1) помогает с обнаружением, закреплением и изъятием электронных носителей информации;

2) помогает с применением технических средств;

3) участвует в обсуждении вопросов, касающихся назначения и производства судебной экспертизы;

4) помогает установить механизм работы электронного носителя информации, и т. п.[2]

Привлекая специалиста, следователь должен проверить его компетентность применительно к конкретному случаю, т. к. обобщенно говорить о «специалисте по компьютерной технике» нельзя ввиду большого разнообразия специальностей: электроника, электротехника, информационные системы и процессы, вычислительная техника, программирование и автоматизация и др.

Специальность, квалификация приглашаемого специалиста зависит от целей и задач осмотра, первоначальных данных о характере преступления. Так, эксперт-криминалист может помочь с обнаружением и сбором традиционных доказательств (например, слабо видимых следов пальцев рук на клавиатуре), а бухгалтер (аудитор) может оказать содействие специалисту-программисту в обнаружении информации в специальных бухгалтерских программах.

---

[1] Старичков М. В. Электронные носители как источники криминалистически значимой информации // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск, 2019. С. 48.

[2] Пастухов П. С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества: монография / под ред. О. А. Зайцева. М. : Юрлитинформ, 2019. С. 78.

На практике увеличить эффективность проводимого осмотра позволяет приглашение следователем к участию в следственном действии владельца электронного носителя информации, сетевого или системного администратора или программиста организации, которые знают особенности эксплуатации осматриваемых компьютеров, схему их соединения и т. д.[1]

В ходе осмотра в зависимости от конкретных обстоятельств могут использоваться различные тактические приемы:

– «от центра к периферии», причем «центром» (отправной точкой осмотра места происшествия) выступает конкретный компьютер, а дальнейшее движение осматривающих должно быть направлено в сторону периферийных и иных устройств;

– «от периферии к центру» (в центре находится самый важный объект – сервер сети).

В целом на практике осмотр обычно начинают с того участка (узла) места происшествия, который содержит наиболее важную криминалистическую информацию (например, основной компьютер). Но здесь надо учитывать, что от выбора правильной последовательности действий следователя и других участников осмотра зависит сохранность и целостность следов преступления[2].

Проводя инструктаж на подготовительном этапе осмотра, следователь обязательно предупреждает участников следственного действия о том, что нельзя прикасаться к компьютерной технике без его разрешения и выключать электроснабжение.

К действиям, которые следователь должен незамедлительно выполнить по прибытии на место происшествия, относятся следующие:

1) исключить доступ персонала осматриваемой организации, учреждения ко всем компьютерам сети, серверу и иным средствам компьютерной техники, и, как следствие, изменению или повреждению содержащейся там информации;

2) удалить с места осмотра посторонних лиц, которые в нем не участвуют, и разместить их в помещении, исключив возможность использования ими любых средств связи;

3) обеспечить охрану средств компьютерной техники и электрических распределительных щитов, пультов;

4) при наличии локальной компьютерной сети, связывающей компьютеры, отсоединить удаленный доступ к системе извне;

5) установить, не запущена ли на компьютере программа уничтожения информации (при запуске данной программы с помощью специалиста

---

[1] Першин А. Н. Электронный носитель информации как новый источник доказательств по уголовным делам // Уголовный процесс. 2019. № 5. С. 53.

[2] Батурин Ю. М. Компьютерная преступность и компьютерная безопасность : учебное пособие. М. : Юридическая литература, 2020. С. 66.

предпринять действия по ее приостановлению или отмене, в том числе отключить компьютер от питания)[1].

Осмотр проводится в присутствии не менее двух понятых с фиксацией следственного действия в протоколе. Возможность производства фото- или видеосъемки законом предусмотрена и требует последующего приложения к протоколу фототаблиц, видеозаписи.

Далее рассмотрим тактические вопросы изъятия электронных носителей, необходимость в котором возникает при проведении обыска и выемки и других следственных действий.

Согласно п. 1 ч. 1 ст. 164.1 УПК РФ изъятие электронных носителей осуществляется лишь после вынесения следователем постановления о назначении судебной экспертизы в отношении электронных носителей информации. Указанное законодательное положение не соответствует установленному порядку назначения судебных экспертиз в связи с тем, что на практике следователь не может принять решение о назначении экспертизы и вынести постановление о ее назначении без указания объектов, направляемых на исследование, и поставить вопросы на разрешение эксперта, не имея в распоряжении материалов, предоставляемых в распоряжение эксперта. А значит норма п. 1 ч. 1 ст. 164. 1 УПК РФ применительно к рассматриваемым объектам не может быть реализована, т. к. к моменту назначения экспертизы объекты уже должны быть изъяты и указаны в постановлении о назначении экспертизы. Другими словами, она может быть проведена только после изъятия электронных носителей.

Рассматриваемая статья предусматривает еще два случая, которые позволяют изъять электронные носители по указанным составам. Так, согласно п. 2 ч. 1 ст. 164.1 УПК РФ изъятие электронных носителей информации производится на основании судебного решения, принимаемого в порядке, установленном ст. 165 УПК РФ. Хотя законодатель не употребляет термина «выемка», думается, что изъятие электронных носителей в основном будет осуществляться в ходе производства выемки. На это указывает то обстоятельство, что на момент изъятия у следователя будут установлены данные о конкретном объекте – электронном носителе из определенного места и у конкретного лица, что позволяет говорить об изъятии в ходе производства именно выемки.

Кроме этого, изъятие электронных носителей допускается, если 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. Таким образом, следователь должен

[1] Губарев Е. К. Информация, содержащаяся на электронном носителе, как вид доказательства по уголовному делу // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов : сборник материалов международной научно-практической конференции. Самара, 2019. С. 160.

установить не только владельца электронного носителя, но и полномочия на владение информацией на носителе, либо в материалах уголовного дела должны содержаться сведения о том, что возможно совершение новых преступлений.

Также следователь имеет право изъять электронный носитель в том случае, если по заявлению специалиста информация может быть утрачена. Такое изъятие производится при соблюдении следующих условий: наличие заявления специалиста, отраженного в протоколе следственного действия, отсутствие возможности копирования информации в связи с ее утратой или изменением; производство копирования в присутствии понятых[1].

На практике изъятие электронных носителей информации, таких как флеш-карты, жесткие диски, телефоны, ноутбуки и т. п., обычно не требует использования специальных знаний, а необходимость их использования возникает при копировании информации[2]. В связи с этим если в ходе производства следственного действия не требуется копирование информации, содержащейся на изъятых предметах, на другие электронные носители, то лицо, проводящее следственное действие, не привлекает специалиста.

На основе проведенного в параграфе исследования считаем возможным сделать следующие выводы. Несмотря на то, что ст. 164.1 УПК РФ внесла существенные изменения в порядок изъятия электронных носителей и копирования информации, а именно: определила его порядок для всех следственных действий; запретила изымать электронные носители информации при производстве следственных действий по уголовным делам о преступлениях в сфере предпринимательской деятельности, за исключением случаев, указанных в ч. 1 ст. 164.1 УПК РФ; установила обязанность следователя привлекать специалиста только при изъятии электронного носителя информации. При этом следователь вправе произвести копирование информации с электронного носителя самостоятельно без его изъятия, по-прежнему остались проблемные вопросы:

– во-первых, действующее уголовно-процессуальное законодательство, к сожалению, не содержит четкой регламентации относительно того, как действовать следователю по преступлениям в сфере экономической и предпринимательской деятельности, когда отсутствует реальная возможность изъятия электронного носителя информации (следует помнить, что по остальным видам преступлений изымать его возможно, но с обязательным участием специалиста);

---

[1] Старичков М. В. Электронные носители как источники криминалистически значимой информации // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. Иркутск, 2019. С. 57.

[2] Васюков В. Ф., Булыжкин А. В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2020. № 6. С. 94.

– во-вторых, следуя п. 1 ч. 1 ст. 164.1 УПК РФ, изъятие электронных носителей возможно только после вынесения постановления о назначении судебной экспертизы в отношении электронных носителей информации. Данная установка не совсем корректна и не согласуется с имеющимися правилами назначения судебных экспертиз. На практике же следователь, не имея в наличии материалов, предназначенных для предоставления в распоряжение эксперта, не сможет фактически ни вынести постановление о назначении экспертизы, ни указать подлежащие исследованию объекты, ни поставить на разрешение перед экспертом интересующие следствие вопросы. Как следствие, положения п. 1 ч. 1 ст. 164. 1 УПК РФ применительно к рассматриваемым объектам не могут быть реализованы, поскольку к моменту назначения экспертизы объекты уже должны быть изъяты и указаны в постановлении о назначении экспертизы;

– в-третьих, формальное выполнение норм закона: в частности, это касается привлечения специалиста «для галочки», не обладающего необходимыми специальными познаниями, имеющего иную специализацию. В идеале специалист должен обладать техническим образованием, а на практике, к сожалению, нередки случаи, когда привлекаются специалисты из других областей (к примеру, трасологи, дактилоскописты), в т. ч. в связи с нехваткой специалистов в сфере информационно-коммуникационных технологий, несоответствием уровня компетентности, недостаточностью опыта и знаний для полноценного, качественного изъятия информации с электронных носителей. Одним из возможных путей решения проблемы стало привлечение не ведомственных специалистов, экспертов, а сотрудников сторонних организаций (системных администраторов, консультантов специализированных магазинов, сотрудников технических отделов, программистов и др.).

Проведенный анализ действующего законодательства позволяет утверждать, что вышеуказанные проблемные моменты требуют корректировки с целью обеспечения единообразия и четкости правоприменительной деятельности, в том числе путем внесения дополнений (относительно ситуаций, когда по преступлениям в сфере предпринимательской деятельности следователь не может изымать электронный носитель, необходимый для расследования) и изменений (чтобы устранить рассогласованность между п. 1 ч. 1 ст. 164.1 УПК РФ и установленным порядком назначения судебных экспертиз) в УПК РФ. Кроме того, следует разработать и закрепить критерии оценки уровня квалификации, достаточности знаний и опыта для специалистов-техников в области работы с электронными носителя информации; закрепить порядок привлечения сторонних специалистов в этой области, чтобы разрешить проблему нехватки ведомственных.

Считаем возможным и целесообразным внести в УПК РФ изменения, которые позволят следователю самостоятельно принимать решение о необходимости привлечения специалиста для осмотра, изъятия электронного носителя информации, копирования информации с него. Включение по-

добной нормы усилит процессуальную самостоятельность следователя в данной области (он сможет принимать соответствующее решение, исходя из конкретной ситуации, вида и процессуальной значимости электронного носителя информации, обстановки проведения соответствующих следственных действий и т. п.), позволит «разгрузить» специалистов.

§ 2. Особенности назначения и производства экспертиз электронных носителей информации

Назначение и производство судебных экспертиз с целью получения доказательств осуществляются на практике достаточно часто в связи с их эффективностью. Применительно к теме нашего исследования имеет смысл подробнее рассмотреть судебную компьютерно-техническую экспертизу (далее – СКТЭ), проводимую в отношении информации, зафиксированной в электронной форме; программного обеспечения; средств компьютерной техники и сетевых технологий.

А. А. Барыгина определяет СКТЭ как «проводимое экспертом исследование информации, зафиксированной в электронной форме, а также технических средств и программного обеспечения компьютерной системы в целях дачи заключения по фактам, имеющим значение для уголовного дела»[1].

В зависимости от характера специальных знаний, используемых в процессе исследования, условно выделяют:

– судебную информационно-компьютерную (в отношении информации, зафиксированной в электронной форме) экспертизу;

– судебную аппаратно-компьютерную (в отношении технических средств компьютерной системы) экспертизу;

– судебную программно-компьютерную (в отношении программного обеспечения компьютерной системы) экспертизу;

– судебную компьютерно-сетевую (в отношении компьютерных средств, реализующих сетевые информационные технологии) экспертизу.

Как отмечает Ю. Н. Соколов, судебная компьютерно-техническая экспертиза направлена на решение идентификационных (когда необходимо сравнить и выявить соответствие, тождество между оригиналом программы и ее копиями на электронных носителях) и диагностических (когда необходимо установить время воздействия на информацию, заключенную на электронном носителе) задач[2].

Е. Р. Россинская, Е. И. Галяшина подчеркивают, что «судебные компьютерно-технические экспертизы производятся в целях определения ста-

---

[1] Барыгина А. А. Доказывание в уголовном процессе: оценка отдельных видов доказательств : учебное пособие. М. : Юрайт, 2019. С. 81.

[2] Соколов Ю. Н. Электронный носитель информации в уголовном процессе // Информационное право. 2019. № 3. С. 25.

туса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним ее исследованием»[1]. Считаем, что авторы верно определяют сущность и назначение рассматриваемого вида судебной экспертизы, однако узкая трактовка СКТЭ как чисто технического исследования компьютера неоправданна. В частности, при расследовании сетевых преступлений важно выявить виртуальные следы преступной деятельности в сети Интернет, установить факт ее осуществления конкретным лицом.

В качестве объекта СКТЭ выступает источник сведений об устанавливаемых фактах (диск с файлами, содержащими информацию), а также материалы уголовного дела, позволяющие установить его обстоятельства (приложенный к протоколу осмотра места происшествия электронный носитель информации).

Объекты СКТЭ:

– родовой (видовой) объект СКТЭ – определенная категория предметов, которые относятся к компьютерно-техническим средствам и обладают общими признаками (например, такие аппаратные объекты, как персональные компьютеры, периферийные устройства, серверы, рабочие станции и т. д.). Данный объект учитывается при назначении рассматриваемой экспертизы;

– конкретный объект СКТЭ – определенное компьютерное средство, для исследования которого проводится рассматриваемая экспертиза, являющееся индивидуально-определенным и неповторимым (жесткий диск). Данный объект учитывается как при назначении рассматриваемой экспертизы (исходя из характера конкретного объекта формулируются вопросы эксперту), так и на этапе ее непосредственного производства (влияет на выбор применяемых методов исследования).

Система родовых (видовых) объектов СКТЭ представлена несколькими классами.

I класс. Аппаратные объекты: настольные и портативные персональные компьютеры, периферийные устройства, сетевые аппаратные средства, мобильные телефоны (могли использоваться для неправомерного доступа к охраняемой законом компьютерной информации); встроенные системы на основе микропроцессорных контроллеров, любые комплектующие всех указанных компонентов. Типичными аппаратными объектами СКТЭ являются: системный блок (в 57 % случаев представляется на СКТЭ; жесткий диск (29 %), магнитооптический диск (20 %); сервер (3 %)).

II класс. Программные объекты: системное программное обеспечение (операционная система, вспомогательные программы, прикладное программное обеспечение). Типичными программными объектами СКТЭ яв-

[1] Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. М. : Проспект, 2019. С. 275.

ляются: системные (операционные системы MS DOS, Windows и др.) и прикладные (Microsoft Office, PhotoShop и др.).

III класс. Информационные объекты: текстовые и графические документы, изготовленные с использованием компьютерных средств; данные в формате мультимедиа; информация в форматах баз данных и других приложений, имеющая прикладной характер (например, когда она является предметом создания вредоносных программ для ЭВМ). Типичными информационными объектами СКТЭ являются: файлы, подготовленные с использованием программных средств; расширение текстовых форматов, графических форматов, форматов баз данных[1].

В соответствии с ч. 1 ст. 195 УПК РФ «следователь, признав необходимым назначение судебной экспертизы, выносит об этом постановление, в котором указываются:

1) основания назначения судебной экспертизы;

2) фамилия, имя и отчество эксперта или наименование экспертного учреждения, в котором должна быть произведена судебная экспертиза;

3) вопросы, поставленные перед экспертом;

4) материалы, предоставляемые в распоряжение эксперта»[2].

Итак, порядок назначения СКТЭ выглядит следующим образом: следователь делает вывод о необходимости назначения СКТЭ при наличии фактических обстоятельств; определяет конкретный вид экспертизы; осуществляет постановку экспертных задач; составляет перечень вопросов для эксперта и подбирает материалы уголовного дела, которые будут ему предоставлены; отбирает объекты экспертизы; процессуально оформляет решение о назначении экспертизы (постановление о назначении, ходатайство в суд); выбирает экспертное учреждение.

Полнота и правильность экспертного исследования и выносимого по его результатам заключения зависит от правильной постановки вопросов эксперту. С учетом специфики рассматриваемой экспертизы у следователя нередко возникают затруднения при их формулировании, т. к. требуются познания технического характера, знание специальной терминологии. В связи с этим следователем должен приглашаться специалист, который поможет корректно, точно и полно составить вопросы для экспертизы. Это очень важный момент, т. к. правильно сформулированные вопросы позволят эксперту дать четкие и полные ответы, которые будут понятны остальным участникам процесса, не обладающим специальными техническим познаниями, а в особенности суду, который будет выносить на их основе судебный акт.

---

[1] Федотов И. С., Смагин П. Г. Электронные носители информации: «вещественные доказательства» или «иные документы»? // Вестник Воронежского государственного университета. Серия: Право. 2020. № 3. С. 197.

[2] Смирнов А. В., Калиновский К. Б. Уголовный процесс : учебник. М. : Инфра-М, 2020. С. 295.

Далее по результатам проведенной СКТЭ следователь обязательно дает оценку заключению эксперта. Однако в большинстве случаев следователи «не решаются» самостоятельно оценивать результаты рассматриваемой экспертизы. Для этого они приглашают специалиста. Но практическая проблема загруженности последних нередко влечет принятие следователем позиции эксперта, изложенной в заключении, как аксиомы, что нарушает требования ст. 85 УПК РФ, касающиеся оценки заключения экспертизы. В связи с этим, как отмечает Э. Р. Гаврилин, «следователь должен самостоятельно осуществить оценку заключения эксперта»[1]. Оценка должна осуществляться с точки зрения относимости, допустимости, достоверности, и, в совокупности со всеми собранными доказательствами, – достаточности для разрешения уголовного дела (ст. 88 УПК РФ).

С целью проверки относимости заключения эксперта к уголовному делу следует проанализировать текст заключения на наличие в нем:

1) указания на постановление о назначении СКТЭ и номера уголовного дела;

2) обстоятельств конкретного уголовного дела;

3) перечня вопросов эксперту по конкретному уголовному делу.

Допустимость заключения эксперта означает то, что оно соответствует требованиям УПК РФ, касающимся порядка назначения и проведения экспертизы (процедуры постановки вопросов эксперту; получения объектов для экспертного исследования), а также оформления заключения.

Важно обращать внимание на такие моменты, как:

– компетентность эксперта, особенно негосударственного (в заключении должны содержаться данные об учебном заведении, специальности эксперта);

– краткое описание объектов экспертизы, их индивидуальные признаки, вид, состояние упаковки;

– характеристику технических средств, которые использовались при проведении СКТЭ;

– демонстрацию методики, которую применил эксперт (на практике специальных методов компьютерной экспертизы нет, и эксперт фактически адаптирует имеющиеся методики к каждому конкретному случаю. Часто в своем заключении эксперты в качестве методики указывают учебно-методическую литературу);

– перечисление способов обеспечения сохранности информации.

Достоверность заключения эксперта – установление действительных связей, отношений и зависимостей между сторонами, свойствами и качествами заключения эксперта.

Важно отметить, что следователь не имеет возможности самостоятельно, без специалиста оценить надежность примененной методики,

[1] Нечаев В. Д. Проблемы использования электронных доказательств в уголовном процессе // Молодой ученый. 2021. № 18 (360). С. 449.

обоснованность полученных результатов и полноту исследования. Он может оценить лишь:

– применение общелогических методов (анализ, синтез и т. д.);

– наличие (отсутствие) в тексте заключения эксперта указания на факт применения отдельных специальных экспертных методов;

– соответствие использованных методических материалов компьютерной тематике;

– последовательность и полноту проведенной экспертизы, ее этапов[1].

На основании вышесказанного считаем возможным заключить, что СКТЭ – это исследование электронной информации, технических средств и программного обеспечения компьютерной системы для решения задач расследования преступлений. Система родовых (видовых) объектов СКТЭ представлена несколькими классами: аппаратные, программные, информационные объекты.

На основании проведенного в параграфе анализа действующего законодательства относительно производства судебных компьютерно-технических экспертиз считаем целесообразным:

– во-первых, судебную компьютерно-техническую экспертизу рассматривать как исследование электронной информации, технических средств и программного обеспечения компьютерной системы для решения задач расследования преступлений;

– во-вторых, заключение эксперта подвергать оценке следователем с точки зрения относимости, допустимости, достоверности, и, в совокупности со всеми собранными доказательствами, – достаточности для разрешения уголовного дела. На практике следователи относятся настороженно к возможности правильной оценки результатов компьютерной экспертизы без приглашения специалиста, но мы согласны, что оценку основных моментов следователь может выполнить самостоятельно с учетом приведенных в исследовании правил.

§ 3. Проблемные вопросы проверки и оценки информации, представленной в электронном виде, в качестве доказательства

Постоянно развивающиеся информационные технологии требуют эффективного использования в уголовном процессе электронных доказательств для раскрытия преступлений. Термин «электронное доказательство» законодателем не раскрывается. Мнения ученых относительно его сущности и характера различаются.

Проверке информации, представленной в электронном виде, посвящена ст. 87 УПК РФ. Отметим, что для проверки доказательств может

[1] Старичков М. В. Электронные носители как источники криминалистически значимой информации // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск, 2019. С. 67.

проводиться их сопоставление, могут исследоваться свойства каждого доказательства в отдельности, устанавливаться источник каждого доказательства, его подлинность, выявляться достоверность сведений, содержащихся в доказательствах.

Сложности при проверке электронной информации:

– большое количество файлов, содержащихся на электронных объектах, при том, что далеко не вся имеющаяся информация имеет значение для уголовного дела;

– наличие возможности скрыть или уничтожить необходимые сведения;

Проверка подлинности источника электронного доказательства сводится к проверке первоисточника, на котором хранилась информация, на предмет невнесения в него модификаций. В таком случае должна существовать возможность идентификации и аутентификации. Под аутентификацией следует понимать возможность проверки целостности и неизменности содержания электронного документа, а под идентификацией – возможность установления лица, от которого такой документ получен[1].

Относимость электронной информации возможно определить при ее воспроизведении с использованием технических средств, а также посредством анализа ее реквизитов. Для этого в большинстве случаев нужна помощь специалиста.

Допустимость, будучи обязательным условием, обращенным к форме доказательства, диктует необходимость соблюдения установленных законом формальных требований. Проверяется законность источника доказательства, обстоятельств формирования доказательства и способа его получения; надлежащее процессуальное оформление доказательства; получение доказательства надлежащим уполномоченным субъектом. Здесь также важно проверить соблюдение условия неизменности информации на носителе (данное условие может быть обеспечено применением специального программного обеспечения).

Как отмечают Н. А. Зигура, А. В. Кудрявцева, «для признания электронных доказательств достоверными:

– они должны быть сформированы в результате корректной работы аппаратных и программных средств;

– они должны быть получены посредством применения научных методов получения цифровой информации;

– цифровая информация должна быть неизменна;

– достоверность должна подтверждаться посредством сопоставления их с другими доказательствами»[2].

---

[1] Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. … канд. юрид. наук. М., 2020. С. 94.

[2] Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательств в уголовном процессе России : монография. М. : Юрлитинформ, 2020. С. 86.

А. С. Александров, С. И. Кувычков считают, «что одна из современных стратегий защиты состоит в подрыве доверия к электронной информации, представляемой в качестве доказательств»[1]. Но любой факт воздействия на файл, проведения различных модификаций цифровой информации устанавливается и проверяется с помощью экспертизы.

Свойство достаточности доказательств характеризует их совокупность с точки зрения убедительности для обоснования какого-либо вывода или процессуального решения[2].

Таким образом, на основании проведенного в параграфе анализа следует отметить, что проверка и оценка электронных доказательств требует не только наличия специальных знаний и их применения на практике, но также и законодательного закрепления действий, производимых с электронными доказательствами.

В связи с этим считаем целесообразным для проверки доказательств проводить их сопоставление, а также исследовать свойства каждого доказательства в отдельности, устанавливать источник каждого из них, его подлинность, выявлять достоверность сведений, содержащихся в доказательствах. В целях проверки подлинности источника электронного доказательства предлагаем подвергать проверке его первоисточник, на котором хранилась информация, на предмет невнесения в него модификаций. Для определения относимости электронной информации рекомендуем подвергать ее обязательному воспроизведению с использованием технических средств, а также подвергать анализу ее реквизиты при участии специалиста.

Таким образом, критерии достоверности электронных доказательств следующие: сформированность в результате корректной работы аппаратных и программных средств; использование научных методов получения цифровой информации; неизменность цифровой информации, сопоставимость с другими доказательствами и др. А значит, при определении достаточности электронных доказательств собирать всю имеющуюся на исследуемом электронном носителе информацию необходимости нет.

---

[1] Там же. С. 89.

[2] Александров А. С., Кувычков С. И. О надежности «электронных доказательств» в уголовном процессе // Библиотека криминалиста: научный журнал. 2018. № 5. С. 80.

ЗАКЛЮЧЕНИЕ

В учебном пособии поднимается не решенный до сих пор на законодательном уровне острый вопрос относительно использования информации, представленной в электронном виде (электронных доказательств) в уголовном судопроизводстве, ее правового режима и уголовно-процессуальной формы.

Важность проблемы особенностей использования информации представленной в электронном виде, в качестве доказательств в уголовном процессе, проблем ее правового регулирования обусловлена потребностями практики, которая все чаще использует сведения из электронных источников, непосредственно сами электронные носители информации в процессе доказывания.

До сих пор решены далеко не все проблемы реализации полномочий следователя при производстве следственных действий, направленных на получение и использование компьютерной информации, а статьи, представленные в УПК РФ, лишь повысили их актуальность. При этом подавляющее большинство исследований проводилось правоведами до внесения изменений в законодательство в части трансформации компьютерной информации в процессуальные формы, а те из них, которые были предприняты после принятия данных поправок, затрагивают лишь отдельные аспекты. Так, до сих пор вне поля зрения исследователей остаются проблемные вопросы получения информации об электронных сообщениях, хранящихся на электронных носителях информации. До конца не изучены проблемы изъятия электронных носителей информации и копирования компьютерной информации в контексте положений, получивших закрепление в ст. 164.1 УПК РФ. Таким образом, институт реализации полномочий следователя в части получения и использования компьютерной информации при производстве следственных действий нуждается в дальнейшем совершенствовании.

Кроме того, порядок обращения с электронными доказательствами в действующем уголовно-процессуальном законодательстве не находит должного правового регулирования, тогда как институт уголовно-процессуального доказывания сталкивается с появлением новых способов сбора, использования, оценки и хранения информации, представленной в электронном виде. В подобных условиях необходимо детальное правовое закрепление условий, порядка и последствий использования доказательственной информации по уголовным делам, представленной в электронном виде, чтобы минимизировать ошибки правоприменения на практике.

Несмотря на отмеченную тенденцию постоянного расширения использования информации, представленной в электронном виде, в качестве доказательств, в уголовно-процессуальном законе отсутствует определения таких понятий, как «электронный носитель информации», «электрон-

ное доказательство», четко не закреплен процессуальный порядок получения доказательственной информации на электронных носителях. Указанные недостатки напрямую влияют на качество, результативность предварительного расследования уголовных дел, не дают возможности правильно собрать и оформить доказательства в виде информации на электронных носителях.

Помимо вышеперечисленного немало проблем возникает в процессе установления и сохранения подлинности и целостности доказательственной информации, представляемой в электронном виде, поскольку такие данные достаточно уязвимы.

Сказанное обусловило актуальность темы учебного пособия, необходимость дальнейшего научного осмысления проблем использования информации, представленной в электронном виде.

Считаем возможным сделать следующие основные выводы.

1. В связи с тем, что закон не дает определения понятия «электронный носитель информации», а научные подходы очень разнообразны, существует острая необходимость его законодательного закрепления, что облегчит практическое применение рассматриваемого вида доказательств. Определение должно исключать его произвольную интерпретацию и подмену на практике, в связи с чем необходимо дать не техническое описание понятия, а указать его значение как источника доказательств.

Электронные носители информации как источники доказательств в зависимости от конкретной ситуации могут выступать вещественными доказательствами или иными документами. При этом определения понятий «вещественное доказательство» и «иные документы» целесообразно дополнить уточнением, что они могут быть представлены в виде электронной информации.

Если электронный носитель информации был орудием (средством) преступления, был получен в результате преступления, выступил в качестве средства обнаружения преступления и установления обстоятельств уголовного дела, был объектом посягательства, он может быть признан вещественным доказательством. Когда же на первый план выходит информационное содержание, а не физические характеристики электронного носителя, позволяющее установить обстоятельства, подлежащие доказыванию, он признается иным документом.

2. Процессуальный порядок собирания доказательственной информации, представленной в электронном виде, напрямую зависит от вида и особенностей самой информации, что наглядно продемонстрировали приведенные классификации: по возможности доступа к информации третьих лиц; по юридическому механизму правовой защиты информации; по отношению к предмету доказывания; с учетом связи информации с событием преступления.

3. Статья 164.1 УПК РФ внесла существенные изменения в порядок изъятия электронных носителей и копирования информации, а именно: определила порядок изъятия электронных носителей и копирования информации для всех следственных действий; запретила изымать электронные носители информации при производстве следственных действий по уголовным делам о преступлениях в сфере предпринимательской деятельности, за исключением случаев, указанных в ч. 1 ст. 164.1 УПК РФ; установила обязанность следователя привлекать специалиста только при изъятии электронного носителя информации. При этом следователь вправе произвести копирование информации с электронного носителя самостоятельно без его изъятия, однако по-прежнему остались нерешенными следующие проблемные вопросы:

– во-первых, по многим преступлениям в сфере предпринимательской деятельности отсутствует возможность изъятия электронного носителя информации (по некоторым изымать можно, но с участием специалиста). Что делать следователю в случае невозможности изъятия электронного носителя информации – в законе не указано;

– во-вторых, согласно п. 1 ч. 1 ст. 164.1 УПК РФ изъятие электронных носителей осуществляется лишь после вынесения постановления о назначении судебной экспертизы в отношении электронных носителей информации. Это положение рассогласовано с установленным порядком назначения судебных экспертиз в связи с тем, что на практике следователь не может принять решение о назначении экспертизы и вынести постановление о ее назначении без указания объектов, направляемых на исследование, и поставить вопросы на разрешение эксперта, не имея в распоряжении материалов, предоставляемых в распоряжение эксперта. Поэтому норма п. 1 ч. 1 ст. 164. 1 УПК РФ применительно к рассматриваемым объектам не может быть реализована, т. к. к моменту назначения экспертизы объекты уже должны быть изъяты и указаны в постановлении о назначении экспертизы;

– в-третьих, номинальное выполнение норм закона: в частности, это касается привлечения специалиста «для галочки», не обладающего необходимыми специальными познаниями, имеющего иную специализацию. Специалист должен быть как минимум с техническим образованием, а на практике часто приглашаются специалисты из других областей (трасологи, дактилоскописты), в т. ч. в связи с нехваткой специалистов в сфере информационно-коммуникационных технологий, несоответствием уровня компетентности, недостаточностью опыта и знаний для полноценного, качественного изъятия информации с электронных носителей. Одним из возможных путей решения проблемы стало привлечение не ведомственных специалистов, экспертов, а сотрудников сторонних организаций (системных администраторов, консультантов специализированных магазинов, сотрудников технических отделов, программистов и др.).

Вышеуказанные проблемные аспекты требуют корректировки с целью обеспечения единообразия и четкости правоприменительной деятельности, в том числе путем внесения дополнений (относительно ситуаций, когда по преступлениям в сфере предпринимательской деятельности следователь не может изымать электронный носитель, необходимый для расследования) и изменений (чтобы устранить рассогласованность между п. 1 ч. 1 ст. 164.1 УПК РФ и установленным порядком назначения судебных экспертиз) в УПК РФ. Кроме того, следует разработать и закрепить критерии оценки уровня квалификации, достаточности знаний и опыта для специалистов-техников в области работы с электронными носителя информации; порядок привлечения сторонних специалистов в этой области, чтобы разрешить проблему нехватки ведомственных.

Считаем возможным и целесообразным внести в УПК РФ изменения, которые позволят следователю самостоятельно принимать решение о необходимости привлечения специалиста для осмотра, изъятия электронного носителя информации, копирования информации с него. Включение подобной нормы усилит процессуальную самостоятельность следователя в данной области (он сможет принимать соответствующее решение, исходя из конкретной ситуации, вида и процессуальной значимости электронного носителя информации, обстановки проведения соответствующих следственных действий и т. п.), позволит «разгрузить» специалистов.

4. СКТЭ целесообразно рассматривать в качестве исследования электронной информации, технических средств и программного обеспечения компьютерной системы для решения задач расследования преступлений. Система родовых (видовых) объектов СКТЭ представлена несколькими классами: аппаратные, программные, информационные объекты.

Заключение эксперта целесообразно подвергать оценке следователем с точки зрения относимости, допустимости, достоверности, и, в совокупности со всеми собранными доказательствами, – достаточности для разрешения уголовного дела. На практике следователи относятся настороженно к возможности правильной оценки результатов компьютерной экспертизы без приглашения специалиста, но мы согласны, что оценку основных моментов следователь может выполнить самостоятельно с учетом приведенных в учебном пособии правил.

5. Проверка и оценка электронных доказательств требуют не только наличия специальных знаний и их применения на практике, но также и законодательного закрепления действий, производимых с электронными доказательствами. В связи с этим считаем целесообразным для проверки доказательств проводить их сопоставление, а также исследовать свойства каждого доказательства в отдельности, устанавливать источник каждого из них, его подлинность, выявлять достоверность сведений, содержащихся в доказательствах.

В целях проверки подлинности источника электронного доказательства предлагаем подвергать проверке первоисточник доказательства, на котором хранилась информация, на предмет невнесения в него модификаций. Для определения относимости электронной информации рекомендуем подвергать информацию обязательному воспроизведению с использованием технических средств, а также подвергать анализу ее реквизиты при участии специалиста.

Допустимость, будучи требованием, обращенным к форме доказательства, диктует необходимость соблюдения установленных уголовно-процессуальным законом формальных условий. Для этой цели считаем необходимым проверять законность источника доказательства, обстоятельства его формирования и способы его получения; его надлежащее процессуальное оформление; поручать получение доказательства надлежащим уполномоченным субъектом. Здесь также важно проверить соблюдение условия неизменности информации на носителе.

Таким образом, критерии достоверности электронных доказательств – это: сформированность в результате корректной работы аппаратных и программных средств; использование научных методов получения цифровой информации; неизменность цифровой информации, сопоставимость с другими доказательствами и др. А значит, при определении достаточности электронных доказательств собирать всю имеющуюся на исследуемом электронном носителе информацию необходимости нет.

В настоящее время уголовно-процессуальное законодательство содержит комплекс полномочий следователя, позволяющий ему проводить две основные группы следственных действий, направленных на преобразование компьютерной информации в доказательственную. Критериями для разграничения данных групп выступают следующие ключевые факторы:

1. Механизм получения следователем доступа к компьютерной информации. Так, первая группа следственных действий направлена на непосредственное обнаружение и получение следователем компьютерной информации, которую он выявляет в ходе осмотров, обысков и выемок. Получив доступ к ней, следователь должен обеспечить фиксацию данной информации, в том числе – посредством ее копирования. Вторая группа следственных действий (осмотр и выемка электронных или иных передаваемых по сетям электросвязи сообщений; контроль и запись телефонных переговоров; получение информации о соединениях между абонентами и (или) абонентскими устройствами) предусматривает опосредованный характер получения данной информации, находящейся в ведении специальных подразделений правоохранительных органов или иных организаций и учреждений, предоставляющих услуги связи или доступ к сети Интернет. Таким образом, следователь получает эту информацию через «посредников».

2. Познавательная структура следственных действий, образующих первую группу, проста: следователь использует приемы поиска, наблюде-

ния, измерения. По сути, это однородные следственные действия. Что же касается структуры действий, входящих во вторую группу – «налицо» комплексный характер деятельности следователя, включающий в себя взаимосвязанную совокупность приемов и методов, а также самостоятельный «технический этап», протекающий без непосредственного участия следователя. Именно опосредованный характер получения данной информации в ходе осуществления следственных действий второй группы влечет появление в структуре этих следственных действий комплекса познавательных операций и приемов. Данная усложненная структура указанных следственных действий обусловлена потребностью в дополнительном исследовании и проверке компьютерной информации, полученной не лично следователем, а посредством иных лиц.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Нормативные правовые акты и иные официальные документы

1. Конвенция о преступности в сфере компьютерной информации ETS № 185 (заключена в г. Будапеште 23 ноября 2001 г.) // Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru/ (дата обращения: 19.05.2024). Текст : электронный.

2. **Российская Федерация. Законы.** Конституция Российской Федерации от 12 декабря 1993 г. (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Собрание законодательства Российской Федерации. 2014. № 31. Ст. 4398. Текст : непосредственный.

3. **Российская Федерация. Законы.** Гражданский кодекс Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. (ч. I). Ст. 3301. Текст : непосредственный.

4. **Российская Федерация. Законы.** Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Российская газета. 2001. № 249.

5. **Российская Федерация. Законы.** Уголовный кодекс Российской Федерации от 24 мая 1996 г. // Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru/ (дата обращения: 19.05.2024). Текст : электронный.

6. **Российская Федерация. Законы.** О банках и банковской деятельности : Федеральный закон от 2 декабря 1990 г. № 395-1 // Собрание законодательства Российской Федерации. 1996. № 6. Ст. 492. Текст : непосредственный.

7. **Российская Федерация. Законы.** О государственной тайне : Федеральный закон от 21 июля 1993 г. № 5485-1 // Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru/ (дата обращения: 19.05.2024). Текст : электронный.

8. **Российская Федерация. Законы.** Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349. Текст : непосредственный.

9. **Российская Федерация. Законы.** О свободе совести и религиозных объединениях : Федеральный закон от 26 сентября 1997 г. № 3-ФЗ // Собрание законодательства Российской Федерации. 2002. № 23. Ст. 2102. Текст : непосредственный.

10. **Российская Федерация. Законы.** Об актах гражданского состояния : Федеральный закон от 15 ноября 1997 г. № 143-ФЗ // Собрание законодательства Российской Федерации. 1997. № 47. Ст. 5340. Текст : непосредственный.

11. **Российская Федерация. Законы.** О связи : Федеральный закон от 7 июля 2003 г. № 126-ФЗ // Российская газета. 2003. 10 июля. № 135. Текст : непосредственный.

12. **Российская Федерация. Законы.** О коммерческой тайне : Федеральный закон от 29 июля 2004 г. № 98-ФЗ // Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru/ (дата обращения: 19.05.2024). Текст : электронный.

13. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Российская газета. 2006. № 165. Текст : непосредственный.

14. **Российская Федерация. Законы.** О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru/ (дата обращения: 19.05.2024). Текст : электронный.

15. **Российская Федерация. Законы.** О национальной платежной системе : Федеральный закон от 27 июня 2011 г. № 161-ФЗ // Российская газета. 2011. № 139. Текст : непосредственный.

16. **Российская Федерация. Законы.** Об основах охраны здоровья граждан в Российской Федерации : Федеральный закон от 21 ноября 2011 г. № 323-ФЗ // Собрание законодательства Российской Федерации. 2011. № 48. Ст. 6724. Текст : непосредственный.

17. **Российская Федерация. Законы.** О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 28 июля 2012 г. № 143-ФЗ // Собрание законодательства Российской Федерации. 2012. № 31. Ст. 4332. Текст : непосредственный.

18. **Российская Федерация. Законы.** О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 4 марта 2013 г. № 23-ФЗ // Собрание законодательства Российской Федерации. 2013. № 9. Ст. 875. Текст : непосредственный.

19. **Российская Федерация. Законы.** О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 27 декабря 2018 г. № 533-ФЗ // Российская газета. 2018. № 295. Текст : непосредственный.

20. Об утверждении Перечня сведений конфиденциального характера : Указ Президента Российской Федерации от 6 марта 1997 г. № 188 // Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru/ (дата обращения: 19.05.2024). Текст : электронный.

21. Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-I // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1993. № 10. Ст. 357. Текст : непосредственный.

22. **ГОСТ Р 7.0.95-2015.** Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Электронные документы. Основные виды, выходные сведения, технологические характеристики : утвержден и введен в действие приказом Росстандарта от 9 декабря 2015 г. № 2127-ст) : дата введения 2016-07-01. Москва : Стандартинформ, 2017. Текст : непосредственный.

23. Постатейный комментарий к Семейному кодексу Российской Федерации, Федеральному закону «Об опеке и попечительстве» и Федеральному закону «Об актах гражданского состояния» / О. Г. Алексеева, В. В. Андропов, А. А. Бухарбаева [и др.]; под редакцией П. В. Крашенинникова. Москва : Статут, 2012. 656 с. Текст : непосредственный.

II. Учебная и научная литература

1. **Аветисян, А. Д.** Актуальные проблемы досудебного производства : учебное пособие / А. Д. Аветисян. Краснодар : Краснодарский университет МВД России, 2020. 72 с. Текст : непосредственный.

2. **Александров, А. С.** О надежности «электронных доказательств» в уголовном процессе / А. С. Александров, С. И. Кувычков. Текст : непосредственный // Библиотека криминалиста: научный журнал. 2018. № 5. С. 77–80.

3. **Арестова, Е. Н.** Предварительное следствие в органах внутренних дел. Взаимодействие следователя с участниками уголовного судопроизводства : учебник и практикум для вузов / Е. Н. Арестова. Москва : Юрайт, 2023. 167 с. Текст : непосредственный.

4. **Арестова, Е. Н.** Уголовно-процессуальная деятельность полиции : учебное пособие для вузов / Е. Н. Арестова. М. : Юрайт, 2023. 241 с. Текст : непосредственный.

5. **Балашова, А. А.** Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учебное пособие / А. А. Балашова; под ред. Ю. В. Гаврилина, А. В. Победкина. Москва : Академия управления МВД России, 2021. 140 с. Текст : непосредственный.

6. **Балашова, А. А.** Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. … канд. юрид. наук / А. А. Балашова. Москва, 2020. Текст : непосредственный.

7. **Барыгина, А. А.** Доказывание в уголовном процессе: оценка отдельных видов доказательств : учебное пособие / А. А. Барыгина. Москва : Юрайт, 2019. Текст : непосредственный.

8. **Батурин, Ю. М.** Компьютерная преступность и компьютерная безопасность : учебное пособие / Ю. М. Батурин. Москва : Юридическая литература, 2020. Текст : непосредственный.

9. **Быков, В. М.** Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы :

монография / В. М. Быков, В. Н. Черкасов. Москва, 2015. Текст : непосредственный.

10. **Васюков, В. Ф.** Изъятие электронных носителей информации при расследовании преступлений : нерешенные проблемы правового регулирования и правоприменения / В. Ф. Васюков, А. В. Булыжкин. Текст : непосредственный // Российский следователь. 2020. № 6. С. 92–97.

11. **Вершинин, А. П.** Электронный документ: правовая форма и доказательство в суде / А. П. Вершинин. Москва, 2020, 170 с. Текст : непосредственный.

12. **Вехов, В. Б.** Электронные доказательства : проблемы теории и практики / В. Б. Вехов. Текст : непосредственный // Правопорядок: история, теория, практика. 2019. № 4 (11). С. 46–50.

13. **Вилкова, Т. Ю.** Уголовно-процессуальное право Российской Федерации. Практикум : учебное пособие для вузов / Т. Ю. Вилкова. Москва : Юрайт, 2023. 629 с. Текст : непосредственный.

14. **Гаврилин, Ю. В.** Электронные носители информации в уголовном судопроизводстве / Ю. В. Гаврилин. Текст : непосредственный // Труды Академии управления МВД России. 2019. № 4 (44). С. 46–50.

15. **Гареева, Э. Р.** Участие специалиста при изъятии электронных носителей информации / Э. Р. Гареева. Текст : непосредственный // Аллея науки. 2019. № 9. С. 744–748.

16. **Гладышева, О. В.** Актуальные проблемы судебного права : учебное пособие для вузов / О. В. Гладышева. Москва : Юрайт, 2023. 164 с. Текст : непосредственный.

17. **Городов, О. А.** Основы информационного права России / О. А. Городов. Санкт-Петербург : Юридический центр Пресс, 2019. Текст : непосредственный.

18. **Григорьев, В. Н.** Некоторые вопросы использования электронных носителей информации при расследовании уголовных дел / В. Н. Григорьев, О. А. Максимов. Текст : непосредственный // Полицейская деятельность. 2018. № 1. С. 13–19.

19. **Губарев, Е. К.** Информация, содержащаяся на электронном носителе, как вид доказательства по уголовному делу / Е. К. Губарев. Текст : непосредственный // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов : сборник международной научно-практической конференции. Самара, 2019.

20. **Зигура, Н. А.** Компьютерная информация как вид доказательств в уголовном процессе России : монография / Н. А. Зигура, А. В. Кудрявцева. Москва : Юрлитинформ, 2020. Текст : непосредственный.

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

22. **Исмагилов, Р. А.** Использование современных технологий в доказывании по уголовным делам (отечественный и зарубежный опыт) : учебное пособие / Р. А. Исмагилов. Уфа : Уфимский ЮИ МВД России, 2021. 88 с. С. 76–87. Текст : непосредственный.

23. **Карташов, И. И.** Цифровая информация в уголовно процессуальном доказывании: понятие и свойства / И. И. Карташов, О. А. Лесников. Текст : непосредственный // Наука. Общество. Государство. 2020. № 4 (32). С. 73–83.

24. **Ким, А. В.** Отдельные вопросы проведения осмотра и экспертизы электронных носителей информации / А. В. Ким. Текст : непосредственный // Юридические науки. 2019. № 1. С. 151–155.

25. **Краснова, Л. Б.** Электронные носители информации как вещественные доказательства / Л. Б. Краснова. Текст : непосредственный // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 4. С. 254–259.

26. **Кузнецов, П. У.** Основы информационного права учебник для бакалавров : учебник для студентов высших учебных заведений / П. У. Кузнецов. Москва, 2014. Текст : непосредственный.

27. **Кульков, В. В.** Методика предварительного следствия и дознания. Руководство для следователей и дознавателей : практическое пособие / В. В. Кульков, П. В. Ракчеева; под редакцией В. В. Кулькова. 2-е изд., испр. и доп. Москва : Юрайт. 2023. 311 с. Текст : непосредственный.

28. **Лазарева, В. А.** Актуальные проблемы уголовно-процессуального права : учебник для вузов / В. А. Лазарева. Москва : Юрайт, 2023. 434 с. Текст : непосредственный.

29. **Лифанова, Л. Г.** Предварительное следствие в органах внутренних дел : учебное пособие / Л. Г. Лифанова. Ставрополь : Ставропольский филиал Краснодарского университета МВД России, 2020. 222 с. Текст : непосредственный.

30. **Маркелов, А. Г.** Иные документы как доказательства в российском уголовном процессе : дис. … канд. юрид. наук / А. Г. Маркелов. Н. Новгород, 2019. Текст : непосредственный.

31. **Нечаев, В. Д.** Проблемы использования электронных доказательств в уголовном процессе / В. Д. Нечаев. Текст : непосредственный // Молодой ученый. 2021. № 18 (360). С. 449–450.

32. **Орлова, А. А.** Место электронных носителей информации в системе доказательств по уголовным делам / А. А. Орлова. Текст : непосредственный // Молодой ученый. 2019. № 15. С. 287–292.

33. **Пастухов, П. С.** Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества : монография / П. С. Пастухов; под ред. О. А. Зайцева. Москва : Юрлитинформ, 2019. Текст : непосредственный.

34. **Першин, А. Н.** Электронный носитель информации как новый источник доказательств по уголовным делам / А. Н. Першин. Текст : непосредственный // Уголовный процесс. 2019. № 5. С. 50–54.

35. **Решняк, О. А.** Особенности расследования хищений чужого имущества, совершенных с использованием информационно-телекоммуникационных технологий : учебное пособие / О. А. Решняк. Волгоград : Волгоградская академия МВД России, 2021. 60 с. Текст : непосредственный.

36. **Россинская, Е. Р.** Настольная книга судьи: судебная экспертиза / Е. Р. Россинская, Е. И. Галяшина. Москва : Проспект, 2019. Текст : непосредственный.

37. **Рудин, А. В.** Проверка доказательств в российском уголовном процессе / А. В. Рудин. Краснодар : Краснодарский университет МВД России, 2021. 162 с. Текст : непосредственный.

38. **Савельева, Н. В.** Проблемы доказательств и доказывания в уголовном процессе : учебное пособие / Н. В. Савельева. Краснодар, 2019. Текст : непосредственный.

39. **Скобелин, С. Ю.** Использование специальных знаний при работе с электронными следами / С. Ю. Скобелин. Текст : непосредственный // Российский следователь. 2019. № 20. С. 30–35.

40. **Смирнов, А. В.** Уголовный процесс : учебник / А. В. Смирнов, К. Б. Калиновский. Москва : Инфра-М, 2020. Текст : непосредственный.

41. **Смолькова, И. В.** Актуальные проблемы охраняемых федеральным законом тайн в российском уголовном судопроизводстве : монография / И. В. Смолькова. Москва : Юрлитинформ, 2014. Текст : непосредственный.

42. **Соколов, Ю. Н.** Электронный носитель информации в уголовном процессе / Ю. Н. Соколов. Текст : непосредственный // Информационное право. 2019. № 3. С. 21–24.

43. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей : учебное пособие / В. Ф. Васюков, Б. Я. Гаврилов, А. А. Кузнецов [и др.]; под общ. ред. Б. Я. Гаврилова. Москва : Проспект, 2019. 160 с. Текст : непосредственный.

44. **Старичков, М. В.** Электронные носители как источники криминалистически значимой информации / М. В. Старичков. Текст : непосредственный // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск, 2019.

45. **Телигисова, С. С.** Законодательные и правоприменительные аспекты получения сведений приватного характера при формировании предмета доказывания по преступлениям, совершенным с использованием современных цифровых и компьютерных технологий / С. С. Телигисова. Текст : непосредственный // Сборник научных статей международных научно-практических конференций. Санкт-Петербург, 2022. С. 256–262.

46. **Телигисова, С. С.** К вопросу о законодательном урегулировании получения доказательств и информации с электронных носителей для расследования преступлений, совершенных с применением информационных, телекоммуникационных и высоких технологий / С. С. Телигисова. Текст : непосредственный // Сборник материалов Международной конференции «Актуальные вопросы науки и образования: отечественный и зарубежный опыт», посвященной 50-летию Уфимского юридического института МВД России / под общей редакцией А. С. Ханахмедова. Уфа, 2021. С. 105–110.

47. **Ткачев, А. В.** Вопросы использования электронных носителей компьютерной информации в уголовном процессе в качестве доказательств иных документов / А. В. Ткачев. Текст : непосредственный // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 3. С. 436–440.

48. **Федотов, И. С.** Электронные носители информации: «вещественные доказательства» или «иные документы»? / И. С. Федотов, П. Г. Смагин // Вестник Воронежского государственного университета. Серия: Право. 2020. № 3. С. 195–198. Текст : непосредственный.

49. **Федюкина, А. Ю.** Следственные действия в современном уголовном процессе России : учебное пособие / А. Ю. Федюкина. Москва : Московский университет МВД России имени В. Я. Кикотя. 2022. 136 с. Текст : непосредственный.

50. **Цоколова, О. И.** Руководство для следователя и дознавателя по расследованию отдельных видов преступлений : учебник в 2 частях. Часть 2 / О. И. Цоколова, Н. Е. Муженская, Г. В. Костылева. Москва : Проспект. 2023. 784 с. Текст : непосредственный.

51. Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / отв. ред. С. В. Зуев. Москва : Юрайт, 2020. 765 с. Текст : непосредственный.

52. **Яновский, Р. С.** Актуальные проблемы производства следственных действий : учебное пособие для вузов / Р. С. Яновский. Москва : Юрайт. 2023. 140 с. Текст : непосредственный.

IV. Эмпирические материалы (материалы судебной, следственной практики и т. д.)

1. Апелляционное определение Верховного Суда Российской Федерации от 4 июня 2013 г. № 41-АПУ13-13сп // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024). Текст : электронный.

2. Дело № 1-657/20. Приговор суда Железнодорожного района г. Ростова-на-Дону от 12 ноября 2020 г. // Архив суда Железнодорожного района г. Ростова-на-Дону. Текст : непосредственный.

3. Дело № 1-25/18. Приговор Ленинского районного суда г. Ульяновска от 19 мая 2018 г. // Архив Ленинского районного суда г. Ульяновска. Текст : непосредственный.

4. Дело № 22-2225/18. Кассационное определение Омского областного суда от 24 мая 2018 г. // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024). Текст : электронный.

5. Дело № 10-2537/18. Апелляционное определение Челябинского областного суда от 30 мая 2018 г. // Судебные и нормативные акты Российской Федерации. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024). Текст : электронный.

6. Дело № 22-455/19. Апелляционное постановление Приморского краевого суда от 2 февраля 2019 г. // Судебные и нормативные акты Российской Федерации. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024). Текст : электронный.

7. Об отказе в принятии к рассмотрению жалобы гражданина Д. А. Прозоровского на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации : Определение Конституционного Суда Российской Федерации от 25 января 2018 г. № 189-О // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024). Текст : электронный.

8. Определение Конституционного Суда Российской Федерации от 11 мая 2012 г. № 814-О // Судебные и нормативные акты РФ. URL: http://sudact.ru/regular/doc (дата обращения: 27.01.2024). Текст : электронный.

Учебное издание

Абдразяпов Ранис Ришатович
(кандидат юридических наук, б/з)
Арсланова Альбина Ринатовна
(кандидат юридических наук, б/з)
Телигисова Софья Сармановна
(кандидат педагогических наук, б/з)
Нуров Мурад Абдусамадович
(б/с, б/з)

ИСПОЛЬЗОВАНИЕ В ДОКАЗЫВАНИИ ИНФОРМАЦИИ, ПРЕДОСТАВЛЕННОЙ В ЭЛЕКТРОННОМ ВИДЕ (ВОПРОСЫ ТЕОРИИИ И ПРАКТИКИ)

Учебное пособие

Редактор Е. А. Карамзина

Подписано в печать 21.06.2024	Выход в свет 28.06.2024
Гарнитура Times	Формат 60х84 1/6
Уч.-изд. л. 3,8	Усл. печ. л. 4
Тираж 50 экз.	Заказ № 28

Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, д. 2

Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, д. 2

ISBN 978-5-7247-1184-5