Федеральное государственное казенное образовательное
учреждение высшего образования
«Восточно-Сибирский институт
Министерства внутренних дел Российской Федерации»

А. А. Балашова

ПРАВОВАЯ ПРИРОДА ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ

Учебное пособие

Иркутск
Восточно-Сибирский институт МВД России
2022

УДК 343.13
ББК 67.629.3
Б20

Печатается по решению редакционно-издательского совета
Восточно-Сибирского института МВД России

Рецензенты:
канд. юрид. наук, доцент Е. А. Новикова;
канд. юрид. наук, доцент А. А. Кригер.

Балашова, Анна Александровна.
Б20 Правовая природа доказательственной информации на электронных носителях : учебное пособие / А. А. Балашова. – Иркутск: Восточно-Сибирский институт МВД России, 2022. – 80 с.

В учебном пособии на основании анализа следственной и судебной практики, а также мнений ученых-процессуалистов представлена классификация информации, содержащейся на электронных носителях. Рассмотрены вопросы, связанные с проблемой цифровизации уголовного процесса и правовой природой доказательственной информации, содержащейся на электронных носителях; с особым видом не общедоступной информации, которую представляет охраняемая федеральным законом тайна, определяющая соответствующий юридический механизм правовой защиты и порядок его преодоления для решения задач уголовного судопроизводства.

Учебное пособие предназначено для курсантов, слушателей, адъюнктов, научно-педагогического состава образовательных организаций МВД России, сотрудников органов внутренних дел Российской Федерации.

УДК 343.13
ББК 67.629.3

© Балашова А. А., 2022
© Восточно-Сибирский институт МВД России, 2022

Оглавление

Введение

Развитие информационно-телекоммуникационных технологий в настоящее время стремительно опережает изменения в законодательстве в данной сфере. Цифровые технологии находят все большее применение при раскрытии и расследовании любых преступлений, в связи с этим на практике все чаще возникают вопросы, связанные с применением электронных носителей информации в доказывании.

«Цифровую среду используют международные террористы, организованная преступность, здесь много потенциальных угроз для общей глобальной безопасности, но и для отдельных стран, их суверенитета и национальных интересов, – подчеркнул Президент Российской Федерации В. В. Путин на заседании Совета безопасности. – XXI век по праву называют временем прорывного развития информационных технологий, они завоевывают буквально все сферы жизни: это новые системы связи, глобальных коммуникаций, так называемый интернет вещей, искусственный интеллект, электронные государственные услуги, цифровая медицина»[1].

Время цифровых технологий предоставило человечеству множество возможностей во всех сферах деятельности. Развитие различных отраслей промышленности, обучение в школах и вузах, проведение конференций, семинаров, приобретение товаров и услуг – везде в настоящее время используются электронные носители информации, цифровизация вошла во все сферы жизнедеятельности. Этот процесс значительно расширяет возможности человечества, но к сожалению, с появлением технической цифровой инфраструктуры модернизируется и совершенствуется преступность. На фоне цифровизации изменился механизм совершения преступлений, возникли новые виды преступлений, требующие, в свою очередь, внесения изменений в действующее законодательство.

В связи с этим роль электронных носителей и информации, имеющей доказательственное значение и содержащейся на них, также возрастает, и правовое регулирование вопросов ее собирания, хранения и использования в процессе доказывания нуждается в детальном совершенствовании.

[1]Путин: в киберпространстве много угроз для глобальной безопасности и суверенитета стран // ТАСС : информ. агентство России : сайт. URL: https://tass.ru/politika/11006783. Дата публикации: 26.03.2021 (дата обращения: 14.04.2022).

Научная гипотеза, выдвинутая нами ранее[2], говорит о том, что процессуальный порядок собирания доказательственной информации на электронных носителях находится в прямой зависимости от комплекса свойств и технических характеристик данных объектов, а также от правового режима отдельных видов информации, содержащейся на них, и носит дифференцированный характер. В этой связи нами была разработана и представлена авторская классификация электронных носителей информации, обусловливающая дифференциацию процессуальной формы собирания доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России. Вместе с тем, для обеспечения полноты и всесторонности рассмотрения вопроса требуется содержательный анализ правового режима отдельных видов информации, содержащейся на электронных носителях, который, в свою очередь, не меньше влияет на процессуальную форму собирания доказательств, чем родо-видовые характеристики самих электронных носителей.

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

Глава 1. Цифровизация уголовного процесса

1.1. Понятие информации и ее цифровизация

Информация неразрывно связана с целями, стоящими перед объектом, ее воспринимающим, равно как и осмысливается и трактуется в аспекте той цели, которая стоит перед воспринявшим[3].

«В широком смысле информация – это новые сведения об окружающем нас мире, которые мы получаем в результате взаимодействия с ним. Информация – это одна из важнейших категорий естествознания (наряду с веществом, энергией и полем)»[4].

«Информация есть отражение в сознании людей объективных причинно-следственных связей в окружающем нас реальном мире»[5] – еще одно определение интересующего нас понятия, больше присущее гуманитарным наукам.

Информация – важнейший атрибут человеческой жизни и общества в целом. Так было всегда. И поскольку понятие "информация" используется во всех сферах научной и интеллектуальной деятельности, в технике, в искусстве, в быту, то можно считать его важнейшей общей категорией бытия и мышления, и, следовательно, философской категорией.

Существует мнение исследователей, что информация – свойство всей материи, и поэтому является полноправной философской категорией. Другие понимают информацию как свойство только человека и общества. Третьи понимают информацию как свойство всей живой материи.

В данном контексте целесообразно обратить внимание на определение понятия информации, содержащееся в Толковом словаре С. И. Ожегова и Н. Ю. Шведовой. В нем информация определяется как:

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

2) сообщения, осведомляющие о положении дел, о состоянии чего-нибудь. Например, научно-техническая и газетная информация; информация средств массовой информации (печать, радио, телевидение, кино)[6].

---

[3] Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учеб. пособие / под ред. Ю. В. Гаврилина, А. В. Победкина. Москва, 2021. С. 10.

[4] Панфилов, И. П., Дырда, В. Е. Теория электрической связи. М.: Радио и связь, 1991. 344 с.

[5] Берг, А. И., Черняк, Ю. И. Информация и управление. М., 1966. 64 с.

[6] Ожегов, С. И., Шведова, Н. Ю. Толковый словарь русского языка. М., 2008. С. 257.

В философском энциклопедическом словаре[7] приведено следующее определение: «Информация (от лат. informatio – ознакомление, разъяснение, представление, понятие):

1) сообщение, осведомление о положении дел, сведения о чем-либо, передаваемом людьми;

2) уменьшаемая, снимаемая неопределенность в результате получения сообщений;

3) сообщение, неразрывно связанное с управлением, сигналы в единстве синтаксических, семантических и прагматических характеристик;

4) передача, отражение разнообразия в любых объектах и процессах (неживой и живой природы)».

Как можно заметить, в настоящее время в научной литературе существует большое количество определений понятия информации.

Если рассмотреть этот вопрос с позиции информатики как науки, которая заключается в проведении исследований и изучении законов, методов и способов накапливания, обработки, передачи информации с помощью электронно-вычислительных машин, а также других компьютерных устройств, то интересующий нас термин «информация» является совокупностью знаний о фактических данных и зависимостях между ними, содержание, присваиваемое данным посредством соглашений, которые распространяются на эти данные[8].

Более общее определение информации, в основу которого положено отражение как свойство материи, было дано А. И. Трусовым, который считал, что «информация охватывает отражение предметов и явлений в человеческом сознании, явлений и процессов друг в друге, вне связи с сознанием»[9].

Еще более широко понимает информацию Р. М. Ланцман. По его мнению, информация – это все то, «что отличает одно явление от другого либо характеризует различные состояния одного явления»[10].

Впервые понятие «информация» на законодательном уровне было закреплено в Федеральном законе от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации»[11], в котором она

---

[7] Философский энциклопедический словарь. М.: Сов. энцикл., 1983. 839 с.

8 Першиков, В. И., Савинков, В. М. Толковый словарь по информатике. М.: Финансы и статистика, 1991. С. 129.

9 Трусов, А. И. Судебное доказывание в свете идей кибернетики // Вопросы кибернетики и право. М.: Наука, 1967. С. 20.

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

[11] Об информации, информатизации и защите информации: Федер. закон от № 24-ФЗ : принят Государственной Думой 25 января 1995 года (утратил силу) // КонсультантПлюс: сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_5887/ (дата обращения: 21.08.2018). Режим доступа: для зарегистрир. пользователей.

определялась как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления».

Заменивший его Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[12] в ст. 2 расширил понятие «информация» и определил ее как сведения (сообщения, данные) независимо от формы их представления.

Анализируя российское законодательство в информационной сфере, отметим, что оно начало формироваться в начале 90-х годов XX века и основывается на положениях следующих основополагающих нормативных актов:

1) Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»;

2) Гражданский кодекс Российской Федерации (части первая, вторая, третья);

3) Федеральные законы:

– от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов»;

– от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– от 07.07.2003 № 126-ФЗ «О связи»;

– от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

– от 27.07.2006 № 152-ФЗ «О персональных данных»;

– от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

4) Указы Президента Российской Федерации:

– от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

– от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»;

– от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации на период до 2030 года» и других.

По мере развития научно-технического прогресса в области информационных технологий, появления цифровых прав их потенциал и реализация постоянно расширяются. Возрастает поток рациональной информации, которая имеет принципиальные отличия от информации, содержащей предполагаемое значение, версию оценочных суждений и даже ненужную информацию[13].

---

[12] Об информации, информационных технологиях и о защите информации: Федер. закон № 149-ФЗ : послед. ред. : принят Государственной Думой 08 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264 (дата обращения: 25.02.2022). Режим доступа: свободный.

[13] Троян, Н. А. Правовая информация как условие трансформации информационного общества в эпоху цифровизации // Право и государство: теория и практика : науч. журн. Королёв. 2020. № 10 (190). С. 134.

С переходом на цифровой сегмент нашей жизни общество столкнулось с новыми понятиями, такими как «цифровая среда», «цифровизация информации», «цифровое сообщество», «цифровизация образования» и др. Изменения, которые в связи с этим происходят в мире, порождают потребности в обучении, овладении цифровыми технологиями и навыками применения их как в повседневной жизни, так и в профессиональной деятельности. Следовательно, как отмечают ученые, процесс цифровизации экономики, образования и любых иных сфер жизни человека предполагает формирование у него цифровой (информационной) культуры, позволяющей грамотно использовать открывающиеся возможности и органично встраиваться в среду информационного общества[14].

В настоящее время в нашем обществе с появлением понятия «цифровая экономика», образовался термин «цифровизация», а вместе с ним – и «цифровизация информации». Тем не менее понятие цифровизации пока не имеет однозначного определения ни в отечественной, ни в западной науке.

Существует мнение, что цифровизация – это новая эпоха, основанную на больших данных («big data») и соответствующих технологиях[15]. Оно вполне заслуживает внимания.

«Преобразование информации в цифровую форму, которое в дальнейшем приводит к оптимизации издержек, появлению новых перспектив развития»[16] – это определение также полно охватывает понятие цифровизации.

Понятие «цифровизация» напрямую связано с понятием «информация», которое, в свою очередь, тождественно понятию «сведения». Цифровые технологии, благодаря которым происходит передача информации, устроены таким образом, что базируются на так называемой логике двоичного кода. В связи с этим привычные ритмы жизни современного мира переходят на другой этап своего развития. Происходит восприятие окружающей действительности визуально, создается новый социальный порядок.

---

[14] Данилова, Л. Н., Ледовская, Т. В., Солынин, Н. Э., Ходырев, А. М. Основные подходы к пониманию цифровизации и цифровых ценностей // Вестник Костромского государственного университета : науч. журн. Кострома: Костромской государственный университет им. Н. Н. Некрасова. 2020. № 2. С. 8.

[15] Никулина, Т. В., Стариченко, Е. Б. Информатизация и цифровизация образования: понятия, технологии, управление // Педагогическое образование в России : международ. науч.-исслед. журн. Екатеринбург: Уральский государственный педагогический университет. 2018. № 8. С. 107–113.

[16] Фомичёва, Т. В., Катаева, В. И. Ценности россиян в контексте цифровизации российской экономики // Уровень жизни населения регионов России : науч.-практич. журн. Москва. 2019. № 2. С. 80–84.

Оцифровка и цифровизация – это два понятия, которые упоминаются в одном контексте с понятием «цифровая экономика». Эти понятия отличаются друг от друга. Процесс перевода информации с физических носителей на цифровые называют оцифровкой (пример – популярные в наше время электронные книги). Цифровизация – более сложный процесс, благодаря которому создается новый цифровой продукт, новые бизнес-модели. То есть имеется в виду область электронных товаров и услуг, основанная на цифровых технологиях.

Процесс оцифровки появился, когда цифровая экономика только начинала зарождаться. Однако в своем развитии цифровая экономика вышла далеко за пределы оцифровки. Использование компьютера для решения задач, традиционно выполняемых вручную или на аналоговых устройствах, стало возможным благодаря цифровизации, но не является достаточным условием для цифровой экономики. Цифровизация как процесс лежит в основе цифровой экономики и делает возможным использование новейших технологий для лучшего и более быстрого выполнения операций, а также для деятельности, которая в прошлом была невозможна.

Процесс цифровизации достаточно важен и направлен на повышение качества жизни населения, а именно:

– доступность и повышение качества сферы медицины и образования;

– повышение комфортности жизни в городах;

– создание платформы с удобными сервисами и госуслугами в цифровом аспекте;

– новые профессии и варианты трудоустройства;

– национальная безопасность, в том числе экономическая, общественная и так далее[17].

В то же время важно соблюдение цифровых защитных мер. Масштабный сбор информации порождает проблемы, связанные с неприкосновенностью частной жизни и безопасностью людей не только в сети, но и за ее пределами. Необходимо обеспечить защиту персональных данных, а также социальную защиту в условиях вытеснения профессий и антимонопольную политику в условиях доминирующего положения крупных фирм, вытесняющих конкурентов, использующих различные инновации.

[17] Хомякова, С. С. Трансформация и закрепление термина «цифровизация» на законодательном уровне // Молодой ученый : международ. науч. журн. Казань. 2019. № 41 (279). Электрон. версия. URL: https://moluch.ru/archive/279/62867. Дата публикации: 11.10.2019 (дата обращения: 20.04.2022). Режим доступа: свободный.

Вопросы для повторения:

1. Понятие информации в различных областях знаний.
2. Понятие цифровизации.
3. На каких нормативных правовых актах основывается законодательство в информационной сфере?
4. Для чего нужна цифровизация информации?

Практическое задание:

1. Подготовить доклад с презентацией на следующие темы:

– «Цифровизация в сфере образования»;
– «Роль цифровизации в современном мире»;
– «Актуальность внедрения цифровизации в уголовный процесс».

1.2. Цифровизация уголовного процесса

Уже более пятнадцати лет в нашей стране уровень обеспеченности судебной системы новым цифровым инструментарием постоянно идет на повышение. Это во многом позволяет повысить открытость судебной системы и облегчить доступ граждан к правосудию.

Доктор юридических наук, профессор А. В. Победкин в одной из своих работ указывает на то, что «уголовное судопроизводство, будучи особой сферой деятельности, сопряженной с решением человеческих судеб, пронизанной нравственными началами больше, чем правовыми, безусловно, не может обходиться без использования научно-технических достижений»[18].

Как считает доктор юридических наук Е. В. Марковичева, обеспечение принципа транспарентности правосудия не только привело к продуктивному использованию современных информационных технологий в деятельности судов, но и породило довольно острую научную дискуссию о возможности цифрового преобразования различных видов судопроизводства[19].

Отношения, которые возникают при внедрении цифровизации в уголовное судопроизводство, затрагивают одновременно права и различные интересы субъектов этих отношений, в связи с чем оптимизация уголовного процесса является одной из приоритетных задач для современного

[18] Победкин, А. В. Этико-аксиологические риски моды на цифровизацию для уголовного судопроизводства (об ошибочности технологического подхода к уголовному процессу) // Вестник Московского университета МВД России : науч. журн. Москва: Московский университет МВД России им. В. Я. Кикотя. 2020. № 3. С. 51.

[19] Марковичева, Е. В. Цифровая трансформация российского уголовного судопроизводства // Правосудие/Justice.. 2020. Т. 2, № 3. С. 91.

российского общества. Повышение эффективности и скорости расследования преступления в уголовном процессе путем цифровизации является основным направлением в упрощении судопроизводства и ведении следственных действий. Определяется это тем, что на сегодняшний день прогресс ушел далеко вперед, появились технологии мгновенной доставки информации, в том числе и документов любой важности. Именно скорость доставки информации является одним из основополагающих факторов в этом вопросе, поскольку это напрямую влияет на то, как быстро будет рассмотрено то или иное процессуальное обращение или будет принято решение о разрешении следственных действий.

В развитии цифрового законодательства в сфере уголовного судопроизводства в значительной мере проявляются корпоративные интересы по уголовным делам о преступлениях в сфере предпринимательской деятельности[20], считает доктор юридических наук, профессор В. Н. Григорьев.

Стоит сказать и о том, что преступность также переходит на использование информационных технологий, что сказывается на характере преступлений и их количестве в информационной сфере. Несмотря на происходящие изменения в качественных характеристиках современной преступности, связанных с использованием при совершении преступлений информационных и коммуникационных технологий, уголовно-процессуальное законодательство Российской Федерации долгое время оставалось не восприимчивым к данной очевидной тенденции. Это является большим упущением современного российского судопроизводства[21].

На данную проблему обращал внимание и Министр внутренних дел Российской Федерации генерал-лейтенант полиции В. А. Колокольцев, а конкретно – на то, что, учитывая масштабы распространения киберпреступлений, разнообразие схем и методов их совершения, отсутствие единых алгоритмов выявления и раскрытия, добиться кардинального улучшения ситуации мерами исключительно организационного и оперативно-розыскного характера не представляется возможным[22].

---

[20] Григорьев, В. Н. Тенденции и проблемы развития законодательства в области информационных технологий, регулирующего уголовное судопроизводство //сетевое издание «Академическая мысль». 2019. № 3 (8). С. 58.

[21] Гаврилин, Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России : науч.-практич. журн. Москва. 2017. № 4 (44). С. 46.

[22] Балашова, А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. … канд. юрид. наук. Москва, 2020. С. 5.

Анализ законодательства позволяет сделать вывод, что происходящие в настоящее время в сфере уголовного процесса изменения, вызванные внедрением информационно-цифровых технологий, в целом не имеют системного характера и не провели к институциональным реформам уголовного процесса.

В настоящее время растет общая тенденция, направленная на урегулирование цифровых отношений в сфере уголовного судопроизводства. Кроме этого, в Государственную Думу вносятся предложения о закреплении таких новейших технических разработок, как полиграф, видеоконференцсвязь, тензометрическая платформа для оценки стрессового психофизического состояния человека, система для ведения «электронных» уголовных дел, видеопротокол, «электронный судья», технология «блокчейн» и криптовалюты[23].

В связи с разнообразием цифровых возможностей, упрощением коммуникаций, повышением процессуальной активности происходит расширение состязательных начал, равных возможностей стороны обвинения и защиты, в том числе в доказывании обстоятельств, имеющих значение для уголовного дела.

При этом перед цифровизацией уголовного процесса стоит не одна, а сразу несколько важных задач. Одна из них – упростить волокиту и повысить коэффициент полезного действия сотрудника органов внутренних дел. Под этим подразумевается переход на более современные технологии, в том числе на электронное судебное производство. Данные меры позволят сэкономить время сотрудника органов внутренних дел, прокуратуры на доставку документа в вышестоящие инстанции, то есть в суд или непосредственному руководителю. Также в теории должна повыситься скорость рассмотрения, а следственно, и ответа на процессуальные документы и запросы, поскольку доставка этих документов станет мгновенной. Поскольку каждое уголовное дело должно рассматриваться очень тщательно, должны приниматься во внимание все мелкие детали психологии и поведения человека, как пострадавшего, так и подозреваемого.

Цифровизация уголовного судопроизводства должна происходить постепенно, поскольку в Российской Федерации нет большого наработанного опыта в сфере электронного документооборота, а электронное судебное

[23] Медведева, М. О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: автореф. дис. ... канд. юрид. наук. Москва: Московский университет МВД России имени В. Я. Кикотя, 2018. С. 19.

производство практически не практиковалось. Поэтому стоит внедрять такую практику постепенно с учетом опыта наших западных коллег. Существует мнение, что российское право в этом отношении явно отстает от зарубежного. Это подтверждается практикой. К примеру, в Великобритании еще в 1993 году впервые судом было рассмотрено дело, где преступление было спроецировано 3D-голограммой, присяжные и судья увидели все обстоятельства преступления в мельчайших подробностях. Как позже отмечал один из присяжных, у него создалось чувство, как будто он сам сидел за кустом и наблюдал за всем произошедшим воочию. По комментариям видных прокуроров и адвокатов, а также ученых-процессуалистов Великобритании, такой подход к делу в разы повышает эффективность и правомерность вынесения приговора, улучшает восприятие всех участников дела и открывает новые возможности как для стороны обвинения, так и для защиты. По отметкам адвокатской палаты, мы должны опираться прежде всего на австрийский и германский опыт, поскольку в этих странах уже завершился переход на электронный документооборот, и у нас схожие правовые системы.

Стоит обратить внимание на то, что отправным моментом цифровизации уголовного процесса должны стать отношения, которые инициируют его начало. То есть первыми цифровыми процессуальными документами должны стать:

– заявление о преступлении;

– явка с повинной;

– постановление прокурора о направлении соответствующих материалов в органы предварительного расследования для решения вопроса об уголовном преследовании;

– или сообщения о совершенном либо готовящемся преступлении, полученные из иных источников[24].

Также поводом к возбуждению уголовного дела должна восприниматься информация о преступлении, которое находится на стадии планирования, при условии обличения ее в перечисленные выше процессуальные формы.

Важно, что если заявление или явка с повинной поступают в качестве заявления в правоохранительные органы в устном виде, то аналогично

[24] Новолодский, Ю. М. Цифровизация уголовного судопроизводства // Федеральная палата Адвокатов Российской Федерации : сайт. URL: https://fparf.ru/polemic/opinions/tsifrovizatsiya-ugolovnogo-sudoproizvodstva/ (дата обращения: 21.09.2021). Режим доступа: свободный.

остальным документам, инициирующим производство по уголовному делу, они должны быть полностью отражены в цифровом поле. Поскольку именно зафиксированные в какой-либо процессуальной форме поводы к возбуждению уголовных дел являются «импульсом» к реальному возбуждению уголовно-процессуального судопроизводства, именно данная стадия должна стать отправной точкой цифровизации.

С другой стороны, в настоящее время, когда происходит поэтапное внедрение цифровых технологий в уголовное судопроизводство России, прослеживаются помимо благоприятных и нужных результатов ряд проблем, связанных с переводом процессуальных документов в цифровой формат:

– дублирование информации на бумаге (двойная работа);

– получение недостоверной, случайной информации;

– отсутствие систем надежной защиты персональных данных;

– трудности выявления, пресечения и предупреждения хакинга и кибершпионажа;

– отсутствие общей цифровой платформы;

– несовместимость и разрозненность имеющегося программного обеспечения; низкий уровень цифрового развития (особенно в сельской местности);

– недостатки правового регулирования[25].

В этой связи правильным будет сказать, что на сегодняшний день в УПК РФ упоминаются электронные носители информации в следующих статьях:

– процессуальные документы могут быть выполнены электронным способом (ч. 2 ст. 474);

– приложением к протоколу следственного действия может выступать информация на электронных носителях (ч. 8 ст. 166);

– применяются фотографирование, аудио- и видеозапись и иные технические средства (ст. 106, 186, 189);

– в качестве вещественных доказательств могут выступать документы на электронных носителях (ч. 4 ст. 81);

– следователем по решению суда могут быть проведены осмотр и выемка электронных сообщений или передаваемых по сетям электросвязи сообщений (ч. 7 ст. 185);

[25] Чурикова, А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник Саратовской государственной юридической академии : науч. журн. Саратов. 2021. № 6 (143). С. 212.

– исполнительный лист вместе с копией приговора, определения, постановления суда может направляться судом для исполнения судебному приставу – исполнителю в форме электронного документа, подписанного судьей усиленной квалифицированной электронной подписью в порядке, установленном законодательством Российской Федерации (ч. 2 ст. 393);

– возможно получение потерпевшим или его законным представителем отдельных видов информации на электронных носителях (ч. 5.1 ст. 42).

Доктор юридических наук, профессор, профессор кафедры уголовно-процессуального права Московского государственного юридического университета имени О. Е. Кутафина (МГЮА) Л. Н. Масленникова и кандидат юридических наук Т. Ю. Вилкова справедливо отмечают, что в настоящее время планируется дальнейшее развитие применения интернет-технологий в российском уголовном судопроизводстве. Президиум правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности 4 февраля 2019 года определил 25 приоритетных жизненных ситуаций, для которых к 2021 году будут созданы суперсервисы – комплексы цифровых госуслуг, в том числе суперсервисы для подачи заявлений в правоохранительные органы онлайн, для цифрового исполнительного производства и осуществления правосудия с использованием интернет-сервисов[26].

Также Л. Н. Масленникова, работая над одним из исследований, пришла к выводу, что начальный этап уголовного судопроизводства, имеющий своим назначением обеспечить доступ к правосудию, нуждается в правовом регулировании использования электронных документов, электронного взаимодействия населения и государственных органов, а также государственных органов между собой[27].

Стоит отметить еще один важный момент эффективного использования оборудования и программного обеспечения: в ходе цифровизации начальных

[26] Вилкова, Т. Ю., Масленникова, Л. Н. Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов – к электронному уголовному делу // Вестник Пермского университета. Юридические науки : науч. журн. Пермь: Пермский государственный национальный исследовательский университет. 2019. Вып. 46. С. 736.

[27] Масленникова, Л. Н. К вопросу о первых результатах реализации научного проекта № 18-29-16018 «Концепция построения уголовного судопроизводства…, обеспечивающего доступ к правосудию в условиях развития цифровых технологий» // Lex Russica (Русский закон) : науч. юрид. журн. Москва: Московский государственный юридический университет им. О. Е. Кутафина. 2020. Т. 73. № 1. С. 74.

стадий уголовного судопроизводства это будет позволять проводить точную фиксацию времени обнаружения процессуальных поводов к возбуждению уголовных дел. В свою очередь, это позволит организовать строгий контроль за соблюдением должностными лицами сроков процессуального реагирования на полученный повод о возбуждении уголовного дела, а также анализировать и давать более объективную оценку эффективности в организации уголовного преследования лиц, подозреваемых в подготовке или совершении преступлений.

Мы подразумеваем, что в рамках электронного уголовного дела будет возможен обмен любой процессуальной информацией между участниками уголовного судопроизводства: в электронном виде направляются жалобы, заявляются ходатайства и отводы, передаются копии соответствующих процессуальных документов и т.д. Автоматически могут исчисляться сроки производства по делу, за определенное время до истечения сроков соответствующие участники процесса об этом уведомляются.

В электронном уголовном деле может быть предусмотрен сервис расположения всех материалов дела в хронологическом порядке. Материалы всех процессуальных и следственных действий должны размещаться на электронном портале не позднее следующего рабочего дня с момента их окончания.

В целом цифровизация судопроизводства должна решить сразу несколько проблем в реализации уголовного процесса нашего государства. Одно из самых важных результатов, на наш взгляд, будет возможность разгрузить практических работников следственных органов, суда и прокуратуры, что приведет к повышению эффективности труда людей. Также это откроет новые возможности для более точного отслеживания времени процессуальных действий. И это только самые явные плюсы. Но не стоит забывать, что все эти меры дадут ощутимый эффект только при условии постепенно внедрения, это должно реализоваться путем поэтапной реформы. На каждом этапе этой реформы нужно будет учитывать все трудности, которые могут возникнуть при ее реализации, главное – это учесть подготовленность людей к использованию цифровых технологий. Здесь стоит учитывать опыт наших западных коллег, которые более прогрессивны в этом плане. Возможно, при подготовке реформы, а также для практического анализа того, как будет влиять каждый этап на уголовно-процессуальную систему в целом, стоит начать с одного или нескольких «экспериментальных» федеральных субъектов, которые станут

своеобразными полигонами проб и ошибок, что позволит не допустить эти же ошибки в масштабах целой страны. Такая практика, к слову, уже использовалась в нашем государстве. Стоит сказать отдельно о важности именно поэтапного и максимально плавного внедрения цифровизации в уголовный процесс и отметить, что в случае неудачи весь позитивный уголовно-процессуальный опыт будет потерян, и это может сильно усложнить все процессуальные действия, что на несколько лет приведет к неэффективности уголовно-процессуальной системы.

В связи с этим процесс цифровизации уголовного судопроизводства должен базироваться на единой платформе, связывающей не только все этапы производства по делу, но и должностных лиц любого из ведомств, осуществляющих определенные этапы этой деятельности. Такая площадка должна соответствовать нормативной базе, быть доступной для всех участников процесса, права и интересы которых затрагиваются рассматриваемой деятельностью. Платформа должна представлять собой гибкую цифровую систему, обеспечивающую сохранность тайны производства с учетом ряда параметров, включая следственную тайну, защиту чести и достоинства человека, его права на неприкосновенность частной жизни, семейную и иную охраняемую законом тайну. Но по другим параметрам она должна быть доступна в установленных законом рамках фигуранту этого процесса, его адвокату и представителю. Кроме того, по определенным параметрам, соответствующим закону, эта платформа также должна быть доступна другим лицам для проведения исследований и обобщения практики уголовного судопроизводства, средствам массовой информации, предоставляющим общественности доступ к информации о ходе производства по определенным делам или в ходе публичных дебатов по определенным правовым вопросам, а также для обеспечения защиты прав человека в сфере уголовного судопроизводства и т.д.

Профессор Л. В. Головко считает, что проявление цифровизации в уголовном судопроизводстве, бесспорно, присутствует и отражается в «трех аспектах, а именно в оцифровке документов, в появлении цифровых следов, и третье – в необходимости закрепления в законе особых «электронных доказательств», то есть расширения перечня видов доказательств»[28].

[28] Головко, Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности : науч. журн. Москва: Московский университет МВД России им. В. Я. Кикотя. 2019. №1. С. 17–21.

Процесс цифровизации уголовного процесса России в настоящее время в периоде интенсивного развития. Анализ зарубежного опыта по этому вопросу, внедрение своих идей и инноваций поможет ученым-процессуалистам в правильном выборе направления развития важного этапа уголовно-процессуальной системы.

Вопросы для повторения:

1. Дать понятие цифровизации уголовного процесса.
2. Какую роль играет цифровизация в уголовном процессе?
3. «Электронное уголовное дело» – перспективы развития.
4. Цифровизация судебной системы.
5. Плюсы и минусы цифровизации уголовного процесса.

Практическое задание:

1. Составить сравнительную таблицу, в которой отразить процесс цифровизации уголовного судопроизводства: что уже сделано, что нужно сделать.
2. Подготовить презентацию на тему «Электронное уголовное дело».

Глава 2. Правовой режим информации, содержащейся на электронных носителях

2.1. Классификация информации, Содержащейся на электронных носителях

Процессуальные проблемы получения дознавателями и следователями сведений, составляющих государственную или иную охраняемую федеральным законом тайну, достаточно тщательно исследованы М. Ю. Тереховым именно применительно к уголовно-процессуальной деятельности органов внутренних дел. По нашему мнению, он является автором наиболее удачного определение понятия «тайна в уголовном судопроизводстве». И трактуется оно как информация или сведения, которые стали известны (или доверены) определенному кругу участников уголовного судопроизводства в связи с их участием при производстве уголовного дела. При этом должен учитываться факт того, что указанные сведения (информация) охраняются уголовно-процессуальным законом от незаконного получения, использования, распространения, а также обеспечивается нейтрализация возможного нарушения прав и законных интересов обладателей указанных сведений[29].

Содержание деятельности, направленной на формирование доказательств в виде сведений на электронных носителях информации, непосредственно зависит от правового режима информации, находящейся на указанных носителях, определяющего наличие ограничений и специальных правовых процедур для формирования на основе данной информации доказательств по уголовному делу.

Как совершенно справедливо в этой связи отмечает А. Н. Яковлев, настоящее состояние правоприменительной практики дает нам понять, что в расследовании преступлений чрезвычайно часто встречается компьютерная информация, которая похожа на тайну. Существует основной принцип отличия такой тайны от фактической (конституционной) тайны. По мнению автора, он заключается в абсолютно разном режиме защиты одинаковой по содержанию информации в равных условиях, но в разном процессе (уголовном, гражданском, административном, арбитражном). «Различать информацию, похожую на тайну, от фактических данных, составляющих тайну, возможно при скрупулёзном знании специализированных нормативных правовых актов,

[29] Терехов, М. Ю. Получение дознавателями и следователями органов внутренних дел сведений, составляющих государственную или иную охраняемую федеральным законом тайну: особенности уголовно-процессуальной формы : автореф. … дис. канд. юрид наук. М., 2010. 33 с.

судебных решений, фактически формирующих прецедент, и умении их сопоставлять»[30].

В этом же контексте Н. Г. Шурухнов и Г. В. Шагара отмечают, что Конституция Российской Федерации предусматривает ограничение права на тайну телефонных переговоров, допускает его только на основании судебного решения и устанавливает запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Такие процессуальные действия обязаны проводиться в строгом соответствии с нормами, установленными федеральными законами[31].

И. Г. Хисматуллиным также поддерживается точка зрения о том, что нелогичным и парадоксальным видится существующий и сформировавшийся на практике порядок проведения осмотра мобильных телефонов, когда в ходе данного процессуального действия, кроме описания внешних признаков, подвергается осмотру информация и иные личные данные владельца телефона, содержащиеся в памяти устройства[32].

В процессе расследования уголовных дел и собирания доказательств органы предварительного следствия, оперативные работники достаточно часто сталкиваются с информацией, относящейся к определенному виду тайны. Практически в каждом уголовном деле имеется изъятый в рамках расследования мобильный телефон, который подлежит осмотру. При этом осматривается не только внешний корпус предмета, но и содержащаяся внутри информация, которая и является практически всегда именно той информацией, ради которой и происходит изъятие аппарата, то есть имеющей доказательственное значение для дела.

Учитывая, что в настоящее время 90 % граждан пользуются смартфонами, то есть телефонами, у которых есть своя операционная система, процессор, оперативная память, информации, хранящейся в них, достаточно много, и она достаточно разнообразна. Иными словами, сейчас мобильное устройство стало полноценной платформой для получения знаний, для работы, игр и т.д. Поэтому сотрудники следственных органов вынуждены осматривать всю имеющуюся в изъятом телефоне информацию, в том числе и личного характера, то есть ту, которая к

---

[30] Яковлев, А. Н. Особенности использования в расследовании преступлений компьютерной информации, похожей на тайну // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений : науч. журн. Воронеж: Воронежский институт МВД России. 2016. № 1. С. 5–11.

[31] Шурухнов, Н. Г., Шагара, Г. В. Процессуальные действия на технических каналах связи как средства, законно ограничивающие конституционное право на тайну телефонных переговоров // Человек: преступление и наказание : науч. журн. Рязань. 2014. № 1. С. 84–86.

[32] Хисматуллин, И. Г. Проблемные вопросы допустимости электронных доказательств в уголовном процессе России // Тенденции развития науки и образования : науч. журн. Самара. 2020. № 65-2. С. 136–139.

уголовному делу не имеет никакого отношения, в целях отыскания нужной им доказательственной информации.

Рассматривая данный вопрос более углубленно, отметим, что помимо осмотра смартфона и имеющейся в нем личной информацией, у следователя возникает необходимость доступа к сведениям, которые составляют тайну и обращение к которым имеет особое нормативное регулирование.

С учетом сказанного, а также в контексте решения задач уголовного судопроизводства, отметим необходимость классификации доказательственной информации, содержащейся на электронных носителях. Ю. В. Шелеговым и В. Г. Шелеговым была предпринята попытка классификации электронных (цифровых) доказательств[33]. Однако полагаем целесообразным произвести классификацию именно по следующим основаниям:

1. По форме представления информация на электронных носителях подразделяется на документированную и недокументированную. Документированная информация представляет собой зафиксированную на материальном носителе информацию с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель. Кроме того, документированная информация определяется как структурированная информация, зафиксированная на носителе.

М. П. Илюшенко, Я. З. Лившиц и Т. В. Кузнецова в своем пособии «Документоведение. Документ и система документации» отмечали, что для документированной информации характерны свойства объективности, достоверности, оптимальности и актуальности[34]. Можно отметить, что в некоторых моментах свойства документированной информации перекликаются с признаками доказательств в уголовном процессе. В частности, объективность и достоверность являются важными составляющими при исследовании доказательств.

Недокументированной информацией считаются те данные, которые не содержат в себе признаков документа, а значит, не имеют соответствующих реквизитов (индивидуальное имя пользователя, логин и подходящий к нему пароль, закрытый и открытый ключи электронной цифровой подписи, идентификаторы), которые автоматически передаются мобильным телефоном при попадании в зону действия оператора связи.

---

[33] Шелегов, Ю. В., Шелегов, В. Г. К вопросу классификации электронных (цифровых) доказательств // Сб. мат-лов XXIV международ. научно-практич. конф. «Деятельность правоохранительных органов в современных условиях». Иркутск: Восточно-Сибирский институт МВД России. 2019. С. 64–68.

[34] Илюшенко, М. П., Лившиц, Я. З., Кузнецова, Т. В. Документоведение. Документ и системы документации : учеб. пособие / под ред. Я. З. Лившиц. Москва, 1977. 88 с.

Уголовно-процессуальное значение приведённой классификации состоит в том, что она имеет определяющее значение при решении вопроса о том, к какому виду доказательств относится соответствующая информация. Так, если доказательственное значение имеет исключительно содержание документированной информации, то она, а точнее сказать, ее носитель, в соответствии с положениями ст. 84 УПК РФ относится к иным документам. Носители же недокументированной информации, а также документированной информации, несущей на себе следы преступления (например, модификации компьютерной информации), относятся к вещественным доказательствам.

2. По критерию доступности информация подразделяется на общедоступную и необщедоступную.

Общедоступная информация – это сведения, которые вполне можно назвать общеизвестными, а также другая информация, доступ к которой не ограничен. Иными словами, доступ к общедоступной информации возможен для неограниченного круга лиц, то есть для ее получения не требуется получение разрешения в какой-либо форме от ее собственника или иного лица. Это новости, сервисы объявлений, информация, размещаемая государственными органами и органами местного самоуправления в информационно-телекоммуникационной сети Интернет в форме открытых данных[35], персональные страницы социальных сетей без

[35] Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных : Постановление Правительства РФ от 10.07.2013 № 583 (вместе с «Правилами отнесения информации к общедоступной информации, размещаемой государственными органами и органами местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных»», «Правилами определения периодичности размещения в информационно-телекоммуникационной сети «Интернет» в форме открытых данных общедоступной информации о деятельности государственных органов и органов местного самоуправления, сроков ее обновления, обеспечивающих своевременность реализации и защиты пользователями своих прав и законных интересов, а также иных требований к размещению указанной информации в форме открытых данных», «Правилами обязательного размещения органами государственной власти субъектов Российской Федерации и органами местного самоуправления общедоступной информации о деятельности органов государственной власти субъектов Российской Федерации и органов местного самоуправления, созданной указанными органами или поступившей к ним при осуществлении полномочий по предметам ведения Российской Федерации и полномочий Российской Федерации по предметам совместного ведения Российской Федерации и субъектов Российской Федерации, переданных для осуществления органам государственной власти субъектов Российской Федерации или органам местного самоуправления, в информационно-телекоммуникационной сети «Интернет» в форме открытых данных») // Государственная система правовой информации : официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201307200001 (дата обращения: 12.10.2021). Режим доступа: свободный.

ограничения прав доступа, иные информационные ресурсы, доступ к которым возможен для неограниченного круга лиц.

Заметим, что право на информацию является одним из важнейших личных прав, непосредственно закрепленных в Конституции Российской Федерации. Так, в ч. 4 ст. 29 Конституции Российской Федерации установлено право каждого на информацию, в связи с этим право на информацию нужно отнести к числу личных конституционных прав. Кроме того, ч. 2 ст. 8 Федерального закона от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации" дает гражданину право на доступ к информации, например на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

При этом, согласно пункту 4 указанного Закона, не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды (экологической информации);

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

4.1) информации, содержащейся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации);

Еще раз уточним понятие «общедоступная информация». Для этого рассмотрим различные правовые нормы.

Так, в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» говорится о понятии общедоступные персональные данные. Согласно данному определению, общедоступные персональные данные – это те персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Анализируя правовые нормы, можно увидеть различные неоднородные определения общедоступной информации.

Так, например, в статье 30 Федерального закона от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг» общедоступной информацией на рынке ценных бумаг признается информация, не требующая привилегий для доступа к ней или подлежащая раскрытию в соответствии с настоящим Федеральным законом[36].

В Лесном кодексе Российской Федерации законодатель указал на то, что к общедоступной информации относится «документированная информация, содержащаяся в государственном лесном реестре, … за исключением информации, доступ к которой ограничен федеральными законами (информация ограниченного доступа)[37]».

Федеральный закон от 20 декабря 2004 года № 166-ФЗ «О рыболовстве и сохранении водных биологических ресурсов»[38] содержит интересующее нас определение в следующей интерпретации: «Государственный рыбохозяйственный реестр представляет собой систематизированный свод документированной информации о водных биоресурсах, об их использовании и сохранении». Документированная информация, содержащаяся в государственном рыбохозяйственном реестре, относится к общедоступной, за исключением информации, доступ к которой ограничен федеральными законами (информация ограниченного доступа) (ч. 3 ст. 43 Закона).

Отметим и Федеральный закон от 30 декабря 2004 года № 218-ФЗ «О кредитных историях»[39], в котором к открытым и общедоступным

---

[36] О рынке ценных бумаг : Федер. закон № 39-ФЗ : принят Государственной Думой 20 марта 1996 года : принят Государственной Думой 20 марта 1996 года : одобрен Советом Федерации 11 апреля 1996 года : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_10148/ (дата обращения: 11.07.2022). Режим доступа: для зарегистрир. пользователей.

[37] Лесной кодекс Российской Федерации : ЛК : Федер. закон № 200-ФЗ (: принят Государственной Думой 8 ноября 2006 года : одобрен Советом Федерации 24 ноября 2006 года (в ред. от 30.12.2021, с изм. и доп., вступ. в силу с 01.03.2022) // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_64299/ (дата обращения: 11.07.2022). Режим доступа: для зарегистрир. пользователей.

[38] О рыболовстве и сохранении водных биологических ресурсов : Федер. закон № 166-ФЗ : принят Государственной Думой 26 ноября 2004 года : одобрен Советом Федерации 8 декабря 2004 года : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_50799/ (дата обращения: 11.07.2022). Режим доступа: для зарегистрир. пользователей.

[39] О кредитных историях : Федер. закон № 218-ФЗ : принят Государственной Думой 22 декабря 2004 года : одобрен Советом Федерации 24 декабря 2004 года // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_51043/ (дата обращения: 11.07.2022). Режим доступа: для зарегистрир. пользователей.

информационным ресурсам относится Государственный реестр бюро кредитных историй.

В Федеральном законе от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации»[40] законодатель указал, что общедоступность официальной статистической информации провозглашена одним из основных принципов официального статистического учета и системы государственной статистики (п. 1 ст. 4).

Понятие «общедоступная информация» упоминается в п. 3 ст. 30 Федерального закона от 25 апреля 2002 года № 40-ФЗ «Об обязательном страховании гражданской ответственности владельцев транспортных средств»[41]: «пользование информационными ресурсами автоматизированной информационной системы является свободным и общедоступным, за исключением информации, составляющей в соответствии с федеральным законом информацию ограниченного доступа».

Федеральный закон от 19 июля 1998 года № 113-ФЗ «О гидрометеорологической службе»[42] содержит норму о том, что информация о состоянии окружающей среды, ее загрязнении и информационная продукция являются открытыми и общедоступными (п. 1 ст. 14).

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»[43] указывает на то, что «в целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в т.ч. справочники, адресные книги)». При этом к общедоступным источникам персональных данных относятся фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных, но исключительно с письменного согласия субъекта персональных данных.

---

[40] Об официальном статистическом учете и системе государственной статистики в Российской Федерации : Федер. закон № 282-ФЗ : принят Государственной Думой 9 ноября 2007 года : одобрен Советом Федерации 16 ноября 2007 года (послед. ред.) // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_72844 / (дата обращения: 25.02.2022). Режим доступа: свободный.

[41] Об обязательном страховании гражданской ответственности владельцев транспортных средств : Федер. закон № 40-ФЗ : принят Государственной Думой 3 апреля 2002 года : одобрен Советом Федерации 10 апреля 2002 года **(**ред. от 01.04.2022) // КонсультантПлюс : сайт. http://www.consultant.ru/document/cons_doc_LAW_36528/ (дата обращения: 11.07.2022). Режим доступа: для зарегистрир. пользователей.

[42] О гидрометеорологической службе : Федер. закон от 19.07.1998 г. № 113-ФЗ : (в послед. ред.) // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/ cons_doc_LAW_19456/ (дата обращения: 11.07.2022). Режим доступа: для зарегистрир. пользователей.

[43] О персональных данных : Федеральный закон № 152-ФЗ : принят Государственной Думой 8 июля 2006 года : послед. ред. : одобрен Советом Федерации 14 июля 2006 года // КосультантПлюс : сайт. URL: http://www.consultant.ru/ document/cons_doc_law_61801/ (дата обращения: 25.02.2022). Режим доступа: свободный.

По требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных[44].

Справедливо подмечено в этой связи А. В. Минбалеевым, что в содержании так называемого информационного права усматриваются две группы прав на информацию, а именно право на информацию публично-правового характера и право на информацию частноправового характера[45].

В этой связи нужно отметить, что важную роль играет способ распространения информации. Если обратимся к истории, то вспомним, что первыми носителями информации в эпоху палеолита были стены пещер. Сначала люди рисовали на стенах пещер, камнях и скалах, такие рисунки и надписи называются петроглифами. Позже материальным носителем информации стали глиняные таблички, а затем восковые таблички. Развиваясь далее, люди изобрели папирус, большое количество информации хранила эта древняя «бумага», достоинство которой можно охарактеризовать в виде надежности хранения информации. Береста – более практичный носитель информации, использовавшийся часто на Руси, а еще позже в Китае была изобретена бумага. Как мы видим, носители информации прошли многовековую эволюцию, и причиной тому было желание людей донести информацию до себе подобных.

Эволюция носителей информации

1)	Стены, камни, скалы (эпоха палеолита)
2)	Глиняные, восковые таблички
3)	Папирус
4)	Береста
5)	Бумага
6)	Фонограф и патефон
7)	Магнитофон
8)	Перфокарты
9)	Жесткий диск
10)	Оптический носитель
11)	Полупроводниковые носители
12)	Облачные хранилища

[44] Там же.

[45] Минбалеев, А. В. Право на информацию: природа и особенности развития в современном мире // Вопросы управления : науч.-информац. журн. Екатеринбург: Российская академия народного хозяйства и государственной службы при Президенте РФ. 2014. № 4 (29), С. 203–207.

При этом в условиях стремительного развития информационно-телекоммуникационных технологий особую актуальность приобрела проблема защиты граждан от несанкционированного, неправомерного сбора их персональных данных, а также злоупотреблений, возможных при сборе, обработке и распространении информации персонального характера, защиты неприкосновенности частной жизни, что, в свою очередь, основано на общепризнанных принципах и нормах международного права, а также международных договорах Российской Федерации, в частности:

– статье 12 «Всеобщей декларации прав человека», согласно которой никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию;

– статье 17 «Международного пакта о гражданских и политических правах», согласно которой никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию;

– статье 16 «Конвенции о правах ребенка», согласно которой ни один ребенок не может быть объектом произвольного или незаконного вмешательства в осуществление его права на личную жизнь, семейную жизнь, неприкосновенность жилища или тайну корреспонденции, или незаконного посягательства на его честь и репутацию, и ряде других.

Необщедоступная информация, содержащаяся на электронных носителях, – это та информация, доступ к которой ограничен согласно нормам законодательства, действующего в настоящее время, также на данное ограничение влияет решение собственника (правообладателя) данной информации. По юридическим правилам, она не может быть доступной для третьих лиц. Необщедоступная информация может быть таковой в силу требований действующего законодательства или на основании решения ее собственника (правообладателя). Полагаем, что для целей уголовно-процессуального порядка получения доказательственной информации, находящейся на электронных носителях, имеет значение и такой вид необщедоступной информации, как информация, ранее удаленная с электронных носителей. Дело в том, что при удалении компьютерной информации с использованием стандартных средств операционной системы физически она продолжает оставаться на соответствующем электронном носителе, а удаляется лишь имя файла из таблицы размещения файлов[46]. В процессе производства судебной

[46] Андриенко, Ю. А. Отдельные аспекты использования информационных технологий и работы с электронными носителями информации в доказывании по уголовным делам // Вестник Сибирского юридического института МВД России : науч. журн. : электр. версия. Красноярск: Сибирский юридический институт МВД России. 2018. № 3 (32). URL: https://cyberleninka.ru/article/n/otdelnye-aspekty-ispolzovaniya-

компьютерной экспертизы возможно восстановление удаленной информации до того, как на ее место будет записана новая информация.

Изложенное наглядно иллюстрируется следующими примерами:

– расследованием по уголовному делу № 1-11/2018 1-155/2017 было установлено, что посредством сотового телефона «LG», принадлежащего гражданину В., осуществлялся выход в сеть Интернет на специальный сайт в период с 20.04.2017 по 27.07.2017. В ходе производства компьютерной экспертизы в представленном в распоряжение экспертов телефоне среди удаленной информации присутствует приложение, поддерживающее jabber-клиент под специальным названием, которое использовалось в интересующий следствие период времени для выхода на специальный сайт, что имеет важное доказательственное значение и опровергает выдвинутую обвиняемым версию защиты[47].

– по уголовному делу № № 1-21/2016. Как видно из заключения эксперта № 25 от 15.01.2015, в памяти телефона «Apple iPhone 5», изъятого у обвиняемого М., обнаружено следующее: приложение для мгновенного обмена сообщениями «ICQ» (версия 5.8), в котором пользователь имеет учетную запись: UIN: «670711591»; привязка данного приложения к номеру № с перепиской (в том числе и удаленной) в приложении «ICQ» (время необходимо корректировать на +4 часа); среди данной переписки имеется переписка с абонентом, использующим НИК UIN: 665713491, в которой имеются сведения о адресах «закладок». Приложение для доступа к социальным сетям «VK»; приложение для управления банковскими счетами ЗАО «Связной Банк» – «QBank». Учетная запись в данном приложении «40817810300052103350». Обнаружена информация о проведенных транзакциях; приложение «jTalk» (версия 0.48.1) – Jabber-клиент для мгновенного обмена сообщениями. В данном приложении пользователь имеет учетную запись, обнаружена переписка, среди данной переписки имеется переписка с абонентом. Вышеприведенные доказательства суд признает относимыми, допустимыми и достоверными доказательствами по делу, не противоречащими друг другу, и, оценивая их в совокупности, считает, что вина обвиняемых С. и М. по данному факту полностью доказана[48].

На сегодняшний день перед международным сообществом стоит задача по поиску разумного компромисса между неприкосновенностью частной жизни и публичным интересом при расследовании преступлений

---

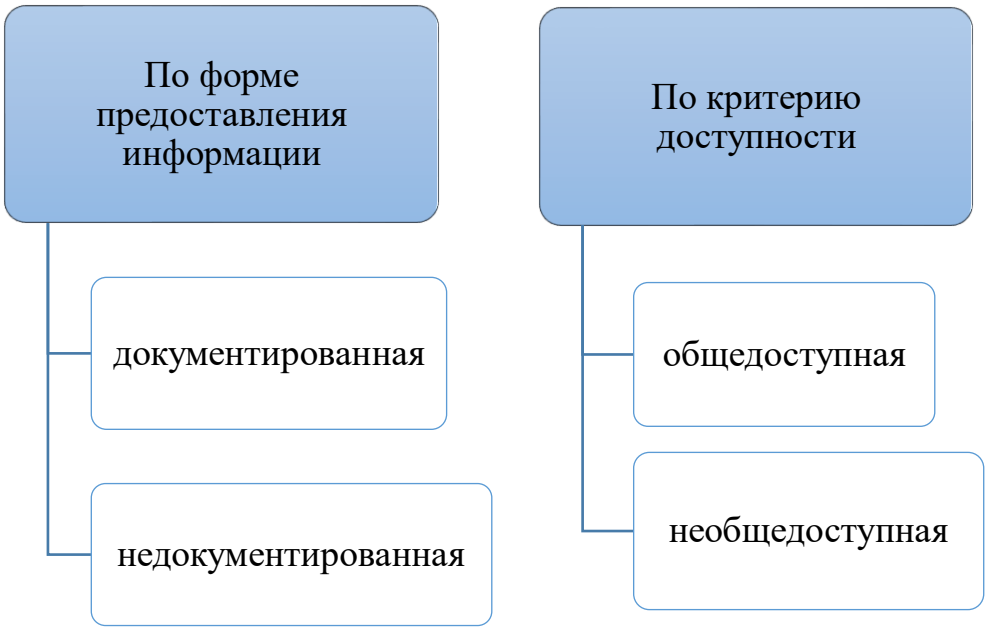
informatsionnyh-tehnologiy-i-raboty-s-elektronnymi-nositelyami-informatsii-v-dokazyvanii-po-ugolovnym (дата обращения: 01.04.2020). Режим доступа: свободный.

[47] Приговор Карпинского городского суда Свердловской области от 25.09.2018 по делу № 1-11/2018 1-155/2017.

[48] Приговор Ленинского районного суда г. Саранска (Республика Мордовия) № 1-21/2016 1-301/2015 от 2 марта 2016 г. по делу № 1-21/2016.

при использовании электронной информации в качестве доказательств по уголовному делу. В существующем уголовно-процессуальном законодательстве необходимо закрепление правовых гарантий, которые будут удовлетворять представления о справедливом правосудии. Должно быть четким изложение обстоятельств, при которых органы предварительного расследования и судебного разбирательства вправе производить процессуальные действия, направленные на обнаружение и сбор электронных доказательств. При этом следует учитывать необходимость соблюдения основных положений неприкосновенности частной жизни граждан, недопущения злоупотреблений в сфере защиты охраняемой законом информации, справедливо считает О. А. Зайцев[49].

КЛАССИФИКАЦИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ



Вопросы для повторения:

1. Какие бывают носители информации?
2. Для чего необходима классификация доказательственной информации, содержащейся на электронных носителях?

[49] Зайцев, О. А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // Журнал зарубежного законодательства и сравнительного правоведения : науч. журн. Москва: Норма. 2019. № 4. С. 54.

3. Какая информация называется документированной? (привести примеры)

4. Какая информация называется недокументированной?

5. Какая информация является общедоступной?

6. Какая информация является необщедоступной?

Практическое задание:

1. Подготовить презентацию с примерами по классификации информации, содержащейся на электронных носителях.

2. Произвести описание информации, полученной в ходе осмотра мобильного телефона, персонального компьютера, в виде фрагмента протокола осмотра.

2.2. Охраняемая федеральным законом тайна как особый вид необщедоступной информации

Мы уже знаем, что существует тайная, конфиденциальная информация, доступ к которой ограничен, соответственно, она нуждается в защите на законодательном уровне и подлежит охране государством.

Законодательство, действующее на сегодняшний день, указывает, что к информации с ограниченным доступом также относится информация, которая не подлежит обнародованию и распространению в средствах массовой информации. Защита конфиденциальной информации сегодня является одним из важнейших факторов создания и обеспечения предпосылок, необходимых для стабильности и дальнейшего развития информационного общества. Она направлена на обеспечение интересов субъектов информационных отношений[50].

Доктор технических наук профессор И. В. Горошко совместно с кандидатом технических наук доцентом В. Н. Лебедевым, занимаясь вопросом правового регулирования передачи служебной информации ограниченного распространения в федеральных органах исполнительной власти, непосредственно обращаются к таким понятиям, как «служебная информация» и «информация ограниченного распространения», а также граничащим с данными понятиями термином «конфиденциальная информация». Очевидно, что, охраняемая федеральным законом тайна, речь о которой пойдет в данной главе, также подпадает под значения и «служебная информация», и «информация ограниченного распространения», и «конфиденциальная информация».

[50] Щадная, М. А., Крючков, М. Д. Конфиденциальная информация: понятие, виды и уровень // Евразийский Союз Ученых (ЕСУ). 3 (12). 2015. С.156.

Термин «конфиденциальный» происходит от латинского confidentia – доверие и первоначально использовался в качестве синонима прилагательного «доверительный» – не предполагающий распространения (например, конфиденциальный (доверительный) разговор)[51].

Отметим, что в некоторых нормативных документах, в справочной литературе и специализированных словарях можно найти другие определения, раскрывающие интересующее нас определение.

Кроме того, вышеназванными учеными отмечается, что конфиденциальность информации относится к специальным правовым режимам, для которых характерны:

– запрет на передачу информации третьим лицам без согласия ее обладателя (за исключением случаев, специально оговоренных в законах);

– возможность обладателя информации самостоятельно решать вопрос о ее конфиденциальности[52].

Целесообразно будет отразить период появления понятия «конфиденциальная информация» в российском законодательстве. Оно появилось уже в Федеральном законе N 24-ФЗ, в котором говорится, что конфиденциальной является документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Стоит обратить внимание, что документированная информация, в зависимости от ее ценности с точки зрения обеспечения государственной безопасности, разделяется на информацию, отнесенную к государственной тайне, и непосредственно конфиденциальную.

Продолжая рассматривать понятие конфиденциальности, обратимся к Указу Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»[53].

---

[51] Горошко, И. В., Лебедев, В. Н. Правовое регулирование передачи служебной информации ограниченного распространения в федеральных органах исполнительной власти // Юридическая наука и правоохранительная практика. 9 (53). 2020. С. 86.

[52] Там же. С. 87.

[53] Об утверждении Перечня сведений конфиденциального характера : Указ Президента Российской Федерации от 06.03.1997 № 188 (в ред. от 13.07.2015) // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_13532/ (дата обращения: 14.03.2022). Режим доступа: свободный.

ПЕРЕЧЕНЬ СВЕДЕНИЙ КОНФЕДЕНЦИАЛЬНОГО ХАРАКТЕРА		
1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные)	2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами, другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну	3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами	5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).	6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.
	7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц.	

В дополнение к таблице важно знать, что:

– в первом пункте существуют исключения, а именно сведения, подлежащие распространению в средствах массовой информации в установленных федеральными законами случаях, не относятся к конфиденциальным;

– во втором пункте речь идет о Федеральном законе от 20 апреля 1995 года № 45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" и Федеральном законе от 20 августа 2004 года № 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства";

– в третьем пункте речь идет о сведениях, составляющих служебную тайну;

– в четвертом пункте под сведениями понимается врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее;

– в пятом – о сведениях, составляющих коммерческую тайну;

– в шестом пункте необходимо понимать, что такое сущность изобретения, полезная модель и промышленный образец; данные понятия содержит Гражданский кодекс Российской Федерации (ст.ст.1351, 1352).

– в седьмом пункте речь идет о сведениях в соответствии с Федеральным законом от 2 октября 2007 года № 229-ФЗ "Об исполнительном производстве".

Данный перечень на сегодняшний день является исчерпывающим.

Имея представление о разновидностях конфиденциальной информации, рассмотрим этот вопрос сквозь призму уголовного процесса.

Как справедливо отмечает С. А. Грачев, имеющиеся в настоящее время несовершенства в нормативно-правовой базе, в которой отсутствуют правила обращения с конфиденциальными сведениями, влекут за собой множество ошибок, допускаемых следователями при расследовании уголовных дел. Кроме того, самое неприятное в данном случае – это признание полученных сведений недопустимыми доказательствами[54]. Прежде всего речь идет о сведениях, разновидности которых упоминались выше, составляющих ту или иную охраняемую законом тайну. Это может быть информация о содержании телефонных переговоров фигурантов дела, о телефонных соединениях между абонентами, переписке

[54] Грачев, С. А. Охраняемая законом тайна в уголовном судопроизводстве: коллизии теории и практики // Юридическая наука и правоохранительная практика : науч. журн. Тюмень: Тюменский институт повышения квалификации сотрудников МВД России. № 1 (51). 2020. С. 76.

посредством почтовой связи, электронной почты или социальных сетей, об обстановке в жилище, о физическом или психическом здоровье подозреваемого (обвиняемого).

Особый вид необщедоступной информации представляет охраняемая федеральным законом тайна, определяющая соответствующий юридический механизм правовой защиты и порядок его преодоления для решения задач уголовного судопроизводства, включает в себя:

– государственную тайну (защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (ст. 2 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне»)[55];

– коммерческую тайну – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду (ст. 3 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне»)[56];

– банковскую тайну – которая содержит в себе информацию, предоставляемую кредитной организацией по поводу операций, счетов, вкладов клиентов и корреспондентов, которым она принадлежит, иные сведения, которые устанавливаются данной организацией (если это не противоречит федеральному закону (ст. 26 Закона РФ от 02.12.1990 № 395-1 «О банках и банковской деятельности»))[57];

– иные профессиональные тайны позволяют трактовать это как информацию, которая доверяется конкретному лицу или становится известной ему в связи с осуществлением им профессиональных обязанностей, перечень которых определен Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» и включает в себя: врачебную, нотариальную, адвокатскую тайну, тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.

---

[55] О государственной тайне : Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.03.2015 № 23-ФЗ) // Собрание законодательства Российской Федерации. 1997. № 41. Ст. 8220; 2015. № 10. Ст. 1393.

[56] О коммерческой тайне : Федер. закон № 98-ФЗ : принят Гос. Думой 9 июля 2004 года : одобрен Советом Федерации 15 июля 2004 года (в послед. ред.) // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/ cons_doc_LAW_48699/ (дата обращения: 20.07.2022). Режим доступа: для зарегистрир. пользователей.

[57] О банках и банковской деятельности: Закон РФ от 02 декабря 1990 года № 395-1 // Ведомости съезда народных депутатов РСФСР. 1990. № 27. Ст. 357.

Врачебная тайна[58] – под ней понимаются сведения, касающиеся обращения граждан за оказанием медицинской помощи, а также которые содержат информацию о состоянии здоровья и диагнозе, иные сведения, полученные при медицинском обследовании и лечении;

адвокатская тайна[59] – любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю;

нотариальная тайна[60] – это та информация, которая стала известной нотариусу в связи с оказанием нотариальных услуг;

налоговая тайна[61] – информация, содержащая полученные налоговым органом (а также органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом) сведения о налогоплательщике, за исключением сведений, предусмотренных ст. 102 Налогового кодекса Российской Федерации;

журналистская тайна[62] – информация, предоставленная кем-либо, то есть лицом, обязующимся хранить ее в тайне, а также источник информации и данные о лице, предоставившем сведения с условием неразглашения его имени;

тайна связи[63] – сведения об абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи; тайна переписки, телефонных переговоров,

---

[58] Об основах охраны здоровья граждан в Российской Федерации : Федер. закон : № 323-ФЗ : послед. ред. : принят Гос. Думой 1 ноября 2011 года : одобрен Советом Федерации 9 ноября 2011 года // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 21.02.2022). Режим доступа: свободный.

[59] Об адвокатской деятельности и адвокатуре в Российской Федерации : Федер. закон : № 63-ФЗ : принят Гос. Думой 26 апреля 2002 года : одобрен Советом Федерации 15 мая 2002 года (ред. от 29.07.2017) // Собрание законодательства Российской Федерации. 2002. № 23. Ст. 2102.

[60] Основы законодательства Российской Федерации о нотариате : утв. ВС РФ 11.02.1993 № 4462-1. Ст. 16 // Государственная система правовой информации : официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 12.03.2022).

[61] Налоговый кодекс Российской Федерации (часть первая) : Федер. закон № 146-ФЗ : принят Гос. Думой 16 июля 1998 года : одобрен Советом Федерации 17 июля 1998 года (ред. от 26.03.2020; с изм. и доп., вступ. в силу с 01.04.2020) // Собрание законодательства Российской Федерации. 1998. № 31. Ст. 3824.

[62] О средствах массовой информации : Закон РФ от 27.12.1991 № 2124-1 // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 7. Ст. 300.

[63] О связи : Федер. закон № 126-ФЗ : принят Гос. Думой 18 июня 2003 года : одобрен Советом Федерации 25 июня 2003 года // Собрание законодательства Российской Федерации. 2003. № 28. Ст. 2895.

почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и почтовой связи.

Приведенный перечень может быть дополнен тайной исповеди, тайной следствия, тайной совещания судей, тайной голосования и пр. Вместе с тем данный перечень наглядно показывает, насколько широк спектр видов подобной информации, имеющей особенности при ее изъятии в процессе досудебного производства.

Судебная практика, связанная с незаконным распространением различных видов тайны, достаточно многообразна и интересна.

В ходе расследования уголовного дела № 1-64/2020 было установлено, что гражданин П. совершил незаконный оборот специальных технических средств, предназначенных для негласного получения информации. Так, гражданин П., проживая совместно с Потерпевшей № 1, преследуя мотив незаконного получения информации, составляющей тайну личной жизни Потерпевшей № 1, решил приобрести свободные для гражданского оборота смарт-часы, обладающие свойством передачи акустической информации с использованием микрофона и встроенным GSM-модулем с целью последующего производства из них специального устройства для негласного получения информации. Действия гражданина П. квалифицированы по ст. 138.1 УК РФ как незаконный оборот специальных технических средств, предназначенных для негласного получения информации (то есть незаконное производство специальных технических средств, предназначенных для негласного получения информации) и по ч. 1 ст. 137 УК РФ как нарушение неприкосновенности частной жизни, то есть незаконное собирание сведений о частной жизни лица, составляющих его личную тайну, без его согласия[64].

Не менее интересным будет следующий пример судебной практики.

Подсудимая Ш. совершила: присвоение, то есть хищение чужого имущества, с использованием своего служебного положения в крупном размере; а также дважды – незаконное использование сведений, составляющих банковскую тайну, без согласия их владельца, из корыстной заинтересованности; присвоение, то есть хищение чужого имущества, с использованием своего служебного положения.

В определенный период времени у гражданки Ш., имеющей доступ к автоматизированной системе Банка и специальному программному обеспечению, которой был достоверно известен порядок заключения, расторжения с физическим лицами договоров вклада, из корыстных побуждений с целью получения незаконного материального дохода, возник преступный умысел на хищение в крупном размере путем

[64] Постановление № 1-64/2020 от 5 февраля 2020 г. по делу № 1-64/2020 Феодосийский городской суд (Республика Крым).

присвоения денежных средств, вверенных ей ПАО «Росгосстрах Банк» в связи со служебным положением, принадлежащих вкладчику ПАО «Росгосстрах Банк» и находящихся на лицевом счете, открытом для учета денежных средств, привлеченных во вклад. Для реализации задуманного гражданка Ш. разработала план совершения преступления, в соответствии с которым она намеревалась, используя свое служебное положение и доступ к автоматизированной системе Банка и специальному программному обеспечению, подыскать информацию о лицевом счете банковского вклада Клиента, на котором размещены денежные средства, принадлежащие Клиенту, используя свой пароль для входа в автоматизированную систему Банка, сформировать расходный кассовый ордер на сумму вклада с учетом начисленных Клиенту процентов, указав в расходном кассовом ордере данные Клиента, не осведомленного о преступных намерениях последней, после чего изъять из кассы, тем самым присвоить, вверенные ей ПАО «Росгосстрах Банк» денежные средства в сумме, указанной в расходном кассовом ордере. Похищенными денежными средствами гражданка Ш. планировала распорядиться по своему усмотрению. Гражданкой Ш. в соответствии с трудовым договором был получен доступ к информации, составляющей банковскую тайну, исключительным собственником которой является ПАО «Росгосстрах Банк» и собственник вклада. В связи с этим гражданка Ш. взяла на себя обязательство о том, что в период ее работы в организации она не имеет права разглашать сведения, которые ей были доверены и стали известны при исполнении служебных обязанностей, хранить тайну об операциях, счетах и вкладах клиентов и корреспондентов ПАО «Росгосстрах Банк», т.е. информации, являющейся банковской тайной. В связи с исполнением своих должностных обязанностей менеджера офисных продаж гражданка Ш. имела доступ к автоматизированной банковской системе Центра финансовых технологий, в которой содержатся данные об операциях, счетах и вкладах клиентов и корреспондентов ПАО «Росгосстрах Банк», в том числе клиентов, заключивших договоры вклада с организацией, что является ее банковской тайной. Действия гражданки Ш. суд квалифицирует по ч. 3 ст. 183 УК РФ – как незаконное использование сведений, составляющих банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по работе, совершенное из корыстной заинтересованности[65].

В ходе расследования уголовного дела было установлено, что гражданин Ф. совершил незаконное разглашение сведений, составляющих налоговую тайну, без согласия их владельца как лицо, которому она стала

[65] Приговор № 1-104/2020 от 29 января 2020 г. по делу № 1-104/2020 Первомайский районный суд г. Новосибирска (Новосибирская область).

известна по службе, из корыстной заинтересованности. В определенный день, находясь возле инспекции ИФНС, специалист разряда Инспекции Федеральной налоговой службы России Ф., действующий в соответствии с должностным регламентом специалиста разряда отдела камеральных проверок № ИФНС России, согласно п. которой он обязан не разглашать сведения, составляющие государственную и иную охраняемую федеральным законом тайну, а также сведения, ставшие ему известными в связи с исполнением должностных обязанностей, проводивший камеральную проверку ООО, сообщил заместителю генерального директора И. указанной фирмы, что контрагенты ООО не представляют налоговую отчетность. В связи с чем гражданин Ф., имея умысел на незаконное разглашение сведений, составляющих налоговую тайну, без согласия их владельца, из корыстной заинтересованности, предложил гражданину И. приобрести за денежное вознаграждение копии ответов на запросы ИФНС России в отношении ООО, а также ответ на запрос ИФНС России в отношении ООО, содержащие сведения о налоговой отчетности, налоговой базе и сумме НДС, осознавая, что передаваемые им сведения составляют налоговую тайну в соответствии с ч. 1 ст. 102 Налогового кодекса Российской Федерации, определяющей, что налоговую тайну составляют любые полученные налоговым органом сведения о налогоплательщике, за исключением сведений, разглашенных налогоплательщиком самостоятельно или с его согласия, об идентификационном номере налогоплательщика, о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения, предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам), предоставляемых избирательным комиссиям в соответствии с законодательством о выборах по результатам проверок налоговым органом сведений о размере и об источниках доходов кандидата и его супруга, а также об имуществе, принадлежащем кандидату и его супругу на праве собственности, и в нарушение требований, предусмотренных ч. 2 ст. 102 Налогового кодекса Российской Федерации, определяющей, что налоговая тайна не подлежит разглашению налоговыми органами. В определенный день гражданин Ф., действуя из корыстной заинтересованности, осознавая, что разглашение сведений, составляющих налоговую тайну, недопустимо и является уголовно наказуемым деянием, пользуясь своим служебным положением, позволяющим получить информацию о юридических лицах, передал

гражданину И. без согласия их владельца копии ответов на запросы ИФНС России в отношении ООО, а также ответ на запрос ИФНС России в отношении ООО, содержащие сведения о налоговой отчетности, налоговой базе и сумме НДС, тем самым разгласив сведения, составляющие налоговую тайну, которые ему стали известны по службе, получив от гражданина И. денежные средства. Действия подсудимого Ф. суд квалифицирует по ч. 3 ст. 183 УК РФ как незаконное разглашение сведений, составляющих налоговую тайну, без согласия их владельца лицом, которому она стала известна по службе, из корыстной заинтересованности[66].

Из приведенных выше примеров судебной практики можно сделать вывод, что правильное определение на предварительном следствии вида охраняемой законом тайны в совокупности с собранными доказательствами влечет утверждение квалификации при рассмотрении уголовного дела в суде.

Анализ эмпирической базы, полученной при опросе и анкетировании сотрудников органов предварительного следствия, показывает, что в 50 % изученных нами уголовных дел в процессе доказывания использовалась информация, относящаяся к коммерческой тайне, в 35 % – к банковской тайне, в 15 % – к тайне переписки, телеграфных сообщений, телефонных переговоров. Значительное количество респондентов (37,3 %) указали, что в ходе расследования была выявлена охраняемая законом информация юридических лиц, содержащаяся на электронных носителях информации, при этом часть из них (21,3 %) указали, что это была коммерческая тайна, 11,3 % указали на тайну частной жизни, 23,3 % – на врачебную тайну, 16,6 % – на тайну семейную, такой же результат был получен на тайну переписки, телеграфных сообщений, телефонных разговоров. По результату опроса сотрудников органов предварительного следствия и дознания установлено, что 88 % опрошенных не усматривают особенностей производства расследования в связи с наличием в уголовном деле информации, относящейся к установленной законом тайне, положительно ответили на данный вопрос 12 % опрошенных сотрудников.

Также установлено, что большинство (65,3 %) респонденты сталкивались в своей практике с изъятием электронных носителей информации, содержащих сведения, относящиеся к охраняемой законом тайне, в процессе расследования по уголовному делу, 34,7 % опрошенных заявили, что не осуществляли подобных процессуальных действий.

Вопрос об отнесении определенной информации к охраняемой законом тайне связи является весьма дискуссионным. Импульс научным

[66] Приговор № 1-561/2011 от 29 сентября 2011 г. Преображенский районный суд (Город Москва).

дискуссиям в этой сфере придает бурное развитие информационно-телекоммуникационных технологий, средств связи, различных интернет-сервисов обмена сообщениями (мессенджеров), электронной почты, социальных сетей и иных информационных ресурсов, на которых происходит обмен сообщениями пользователей[67].

Как уже отмечалось, согласно ч. 2 ст. 23 Конституции Российской Федерации, каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. Данное право закреплено также в п. 1 ст. 8 Конвенции о защите прав человека и основных свобод[68], в ст. 13 УПК РФ, ст. 15 Федерального закона от 17 июля 1999 года № 176-ФЗ «О почтовой связи». Информация, полученная с нарушением установленного законом порядка получения сведений, составляющих тайну связи, признается недопустимым доказательством и не может использоваться в уголовном судопроизводстве. Запрет нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений распространяется в равной степени на операторов почтовой и иных видов связи, должностных лиц органов предварительного следствия и дознания, а также на всех граждан и организации.

При этом следует отметить, что в течение длительного времени наблюдается тенденция расширения предметной области понятия «тайна связи», которая давно вышла за пределы тайны почтовой корреспонденции, телефонных переговоров и телеграфных сообщений, что является общемировым трендом. Так, в статье 7 «Хартии Европейского Союза об основных правах» закрепляются права каждого человека «на уважение своей частной и семейной жизни, своего жилья и своих коммуникаций», охватывающие *«не только... корреспонденцию, но и все иные виды коммуникаций»*[69] *(курсив – авт.)*.

---

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

[68] Конвенция о защите прав человека и основных свобод : заключена в г. Риме 04.11.1950 (с изм. от 13.05.2004) (вместе с «Протоколом [№ 1]» (Подписан в г. Париже 20.03.1952), «Протоколом № 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом № 7» (Подписан в г. Страсбурге 22.11.1984)) // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_29160/ (дата обращения: 26.03.2020). Режим доступа: для зарегистрир. пользователей.

[69] Хартия Европейского Союза об основных правах (Страсбург, 12 декабря 2007 г.) (2016/C 202/02) // КонсультантПлюс : сайт. URL: http://www.consultant.ru/law/podborki/hartiya_evropejskogo_soyuza_ob_osnovnyh_pravah/ (дата обращения: 26.08.2019). Режим доступа: для зарегистрир. пользователей.

Объем сведений, подлежащих конституционно-правовой защите в рамках права на тайну телефонных и иных переговоров, Конституционный Суд Российской Федерации определил следующим образом: Право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления. В силу этого информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям … необходимо получение судебного решения. Иное означало бы несоблюдение требования статьи 23 (часть 2) Конституции Российской Федерации о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения[70].

Значительно сложнее решается вопрос о распространении режима правовой охраны тайны переписки на сообщения, передаваемые посредством сервисов электронной почты, сервисов передачи сообщений, а также социальных сетей.

Поддерживаем точку зрения С. В. Баринова, А. Л. Карлова, А. Н. Яковлева, которые отмечают факт распространения тайны связи, которая закреплена в ст. 63 Закона «О связи», на электронные сообщения и электронную почту. Кроме того, подмечено, что это касается рамок границ технической ответственности, которые принадлежат операторам связи. Выходящая за границы технической ответственности оператора связи, а именно на серверах организаций – собственников информационных ресурсов интернет-сервисов электронной почты, мессенджеров, социальных сетей (например, Google.com, vk.com, и т. п.), а также в информационной системе отправителя и адресата сообщения, информация представляет собой данные, пересылаемые деперсонализированными пользователями сети Интернет в рамках договоренности между собой, об использовании коммуникационных сервисов. Стороны, которые

[70] Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи»: Определение Конституционного Суда РФ от 02.10.2003 № 345-О // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_45175/ (дата обращения: 26.03.2020). Режим доступа: свободный.

пользуются коммуникационным сервисом, могут договориться с его правообладателем об отсутствии какой-либо ответственности за пересылку последним данных. Типовым пользовательским соглашением коммуникационных сервисов, как правило, предусматривается, что они осуществляют обезличенную передачу сообщений пользователей, что исключает распространение на данную информацию правового режима тайны связи. Как только владелец данного сервиса получает указанные данные, он пересылает их оператору связи. Именно в этот момент они подлежат правовой охране как тайна связи. Когда информация появляется у получателя на компьютерном средстве (смартфон), она вновь становится не охраняемыми законом данными, которые получил пользователь сети Интернет. Именно поэтому получать данную информацию органами следствия можно в порядке ст. 86 УПК РФ в ходе следственных действий, и решения суда для этого не требуется.

Особое место в круге информации ограниченного распространения занимает личная тайна. Действующее законодательство не определяет содержание данного понятия. Конституционный Суд Российской Федерации в понятие «частная жизнь» включает ту область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если носит не противоправный характер (определения Конституционного Суда Российской Федерации от 09.06.2005 № 248-О, от 26.01.2010 № 158-О-О и от 27.05.2010 № 644-О-О)[71].

По мнению И. В. Смольковой, личная тайна – информация, которая может содержать в себе сведения о здоровье (болезни, которые считаются постыдными с позиции общественной морали), связях, сопряженных с супружеской изменой, а также о дурных привычках, склонностях, различных пристрастиях, пороках, граничащих даже с нервно-психическими аномалиями; о порочном социальном прошлом гражданина, а также порочащих человека деловых и дружеских связях.

Такой подход, на наш взгляд, во многом допускает смешение понятий медицинской и личной тайны. При этом соглашаемся с отнесением к ней таких скрыто-интимных сторон жизни человека, когда разглашение каких-либо сведений является как нежелательным, так и вредоносным, пагубным с нравственной точки зрения. Так, в рамках расследования уголовного дела № 1-491/2018 установлено, что в ноябре

[71] Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации : Определение Конституционного Суда РФ от 28.06.2012 № 1253-О // Гарант : сайт. URL: https://base.garant.ru/70205530/ (дата обращения: 26.03.2020). Режим доступа: свободный.

2017 года М. пригрозил незаконно распространить сведения о частной жизни потерпевшей, позорящие ее и порочащие ее честь, достоинство, а также подрывающие репутацию, составляющие ее личную тайну, путем размещения ее фотографий интимного характера в открытом доступе в сети Интернет для всеобщего обозрения[72].

В число информации ограниченного распространения входят и персональные данные. Согласно ст. 3 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Следующие примеры судебной практики – также о нарушении частной жизни и личной тайны.

В ходе расследования уголовного дела гражданин А. обвинялся в незаконном собирании и распространении сведений о частной жизни лица, составляющих его личную тайну, без его согласия, при следующих обстоятельствах: обвиняемый А. подобрал мобильный телефон «Samsung A 30», принадлежащий ранее знакомой ему П. У обвиняемого А. возник преступный умысел, направленный на незаконное собирание, а затем распространение сведений о частной жизни знакомой П., составляющих её личную тайну, без согласия последней, а именно сфотографировать из ее мобильного телефона «журнал звонков» и переписку гражданки П. В целях реализации возникшего преступного умысла обвиняемый А. в нарушение ч. 1 ст. 23, ч. 1 ст. 24 Конституции РФ, ст. 12 Всеобщей декларации прав человека, принятой Генеральной Ассамблеей Организации объеденных наций 10 декабря 1948 года, ст. 17 Международного пакта о гражданских и политических правах от 16 декабря 1966 года, введя известный пароль на мобильном телефоне «Samsung A 30», принадлежащем знакомой П., вошел в раздел телефона «журнал звонков» и, используя видеокамеру принадлежащего ему мобильного телефона «Samsung Galaxy J 6», умышленно, без согласия гражданки П. сделал 12 фотографий, содержащих сведения о соединениях. После этого обвиняемый А. вошел в раздел «СМС сообщения», а именно переписку гражданки П., и, используя видеокамеру принадлежащего ему телефона «Samsung Galaxy J 6», умышленно, без согласия П. сделал 5 фотографий, содержащих переписку между П. и гражданином Б. Тем

72 Приговор Ленинского районного суда г. Махачкалы от 17.10.2018 по делу № 1-491/2018.

самым своими преступными действиями обвиняемый А. получил сведения о частной жизни гражданки П., составляющие ее личную тайну, содержащуюся в 17-ти фотографиях. Имея незаконно полученную информацию о частной жизни гражданки П., составляющую ее личную тайну, без ее согласия (4 фотографии, в которых содержались сведения о соединениях и переписке последней), в продолжение реализации преступного умысла, обвиняемый А. умышленно, сообщением передал вышеуказанные фотографии, содержащие личную тайну П. своей знакомой гражданке Д. Таким образом, обвиняемый А. своими умышленными действиями существенно нарушил права своей знакомой гражданки П. на неприкосновенность частной жизни, личной тайны[73].

В другом случае в ходе расследования уголовного дела установлено, что гражданин Б. нарушил неприкосновенность частной жизни, то есть совершил незаконное собирание и распространение сведений о частной жизни лица, составляющих его личную тайну, без его согласия, с использованием своего служебного положения. Гражданин Б. был назначен на должность менеджера офиса продаж и обслуживания салона связи «Мегафон». В своей работе гражданин Б. руководствовался требованиями должностной инструкции, а также действующим законодательством РФ и локальными нормативными актами АО «Мегафон Ритейл».

Согласно ч. 1 ст. 23 Конституции РФ, каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. В силу ч. 1 ст. 24 Конституции РФ, сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. В соответствии со своей должностной инструкцией, гражданин Б. осуществлял обслуживание клиентов салона связи «Мегафон» с помощью специализированной системы ПАО «Мегафон» - биллингового приложения для обслуживания клиентов, а именно «Single Business Management System» (далее SBMS), при этом нес ответственность за разглашение сведений, составляющих служебную и (или) коммерческую тайну АО «Мегафон Ритейл». В один из дней посредством переписки в сети Интернет с использованием мессенджера «Telegram» неустановленное лицо под псевдонимом предложило гражданину Б. за денежное вознаграждение предоставить сведения об абоненте АО «Мегафон Ритейл». Вследствие этого у гражданина Б., находившегося на своем рабочем месте в офисе продаж АО «Мегафон Ритейл», возник преступный умысел на незаконное обогащение путем нарушения неприкосновенности частной жизни ранее ему

[73] Постановление № 1-222/2020 от 15 июля 2020 г. по делу № 1-222/2020 Заднепровский районный суд г. Смоленска (Смоленская область).

незнакомой И. В определенный день в офисе продаж АО «Мегафон Ритейл» гражданин Б., реализуя задуманное, действуя умышленно, из корыстных побуждений, используя свое служебное положение, осознавая, что своими действиями нарушает конституционное право потерпевшей И. на неприкосновенность частной жизни, вопреки воле последней, воспользовавшись открытой учетной записью сотрудника АО «Мегафон Ритейл» С., не осведомленного о его преступном замысле, на служебном компьютере осуществил доступ через специализированную систему АО «Мегафон Ритейл»» (SBMS) к базам данных АО «Мегафон Ритейл», содержащим персональные данные абонента И., а именно гражданин Б. осуществил просмотр и фотосъемку на мобильное устройство «Huawei P20 Lite» личных данных (паспортные данные, сведения о месте регистрации, дата рождения, фамилия, имя и отчество), составляющих личную тайну потерпевшей. Непосредственно после этого гражданин Б., продолжая свои преступные действия, используя мобильное устройство «Huawei P20 Lite», распространил в сети Интернет через мессенджер «Telegram» сделанную им фотографию, содержащую вышеуказанные личные данные И., неустановленному пользователю мессенджера «Telegram» под псевдонимом «Zer2122», за что последний перевел гражданину Б. денежные средства в сумме 200 рублей через платежную систему Яндекс Кошелек. Таким образом, суд квалифицировал действия гражданина Б. по ч. 2 ст. 137 УК РФ как нарушение неприкосновенности частной жизни, то есть незаконное собирание и распространение сведений о частной жизни лица, составляющих его личную тайну, без его согласия, совершенное лицом с использованием своего служебного положения[74].

В ходе расследования уголовного дела № 1-49/2020, было установлено, что гражданин Б. нарушил неприкосновенность частной жизни, то есть незаконно распространил сведения о частной жизни лица, составляющие его личную тайну, без его согласия, а также совершил вымогательство, то есть требовал передачу чужого имущества под угрозой распространения сведений, позорящих потерпевшего. В определенный период времени гражданин Б., осознавая противоправный характер своих преступных действий, действуя умышленно, незаконно, из личных неприязненных отношений и ревности к Потерпевшей № 1, обладая достаточными знаниями в области информационных технологий и навыками пользования техническими устройствами и программными средствами, являясь пользователем сети Интернет, использовал личный мобильный телефон марки «HONOR», Imei-1: №, Imei-2: №, оператора мобильной связи ПАО «МобильныеТелеСистемы», подключенный к

[74] Приговор № 1-77/2020 от 18 мая 2020 г. по делу № 1-77/2020 Фрунзенский районный суд г. Владимира (Владимирская область).

телекоммуникационной сети Интернет, с целью распространения сведений о частной жизни Потерпевшей № 1, составляющих её личную тайну, без согласия последней. Предвидя возможность наступления общественно опасных последствий и желая этого, Б. распространил не менее 5 графических файлов с изображением Потерпевшей № 1 в обнаженном виде, полученных в ходе совместной с Потерпевшей № 1 жизни**,** путем размещения указанных фотографий на странице в социальной сети «ВКонтакте», доступной для просмотра всем пользователям данного интернет-сайта, а также путем направления личными сообщениями пользователям социальной сети «ВКонтакте» указанных фотографий. Также гражданин Б., действуя умышленно, незаконно, из корыстных побуждений, с целью личного обогащения и неправомерного завладения чужим имуществом, под угрозой распространения сведений, позорящих потерпевшую, желая путем вымогательства завладеть денежными средствами, осуществил звонки Потерпевшей № 1, в ходе которых высказывал требования передачи чужого имущества – денежных средств в сумме от 10 000 рублей до 15 000 рублей, принадлежащих Потерпевшей № 1, угрожая в случае отказа распространить сведения, позорящие потерпевшую, порочащие ее честь, достоинство и подрывающие ее репутацию, при этом указанные угрозы Потерпевшая № 1 воспринимала реально.

Действия подсудимого Б. суд квалифицирует:

– по первому эпизоду, по ч. 1 ст. 137 УК РФ как нарушение неприкосновенности частной жизни, то есть незаконное распространение сведений о частной жизни лица, составляющих его личную тайну, без его согласия;

– по второму эпизоду, по ч. 1 ст. 163 УК РФ как вымогательство, то есть требование передачи чужого имущества под угрозой распространения сведений, позорящих потерпевшего[75].

На процессуальную форму собирания доказательственной информации, находящейся на электронных носителях, оказывает ее связь с событием преступления. Н. А. Зигура предлагает по данному основанию следующую классификацию компьютерной информации:

– которая служила орудием совершения преступления (например, различные программы по подбору паролей, вредоносные программы);

– которая сохранила на себе следы преступления (например, любая модификация компьютерной информации);

[75] Приговор № 1-49/2020 от 6 февраля 2020 г. по делу № 1-49/2020 Оренбургский районный суд (Оренбургская область).

– информация, на которую были направлены преступные действия (к ней относится компьютерная информация, которая охраняется законом и может находиться на электронном носителе, в системе или 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.

Автор вышеуказанной классификации обоснованно полагает, что ее значение отвечает цели уголовно-процессуального доказывания – установлению обстоятельств, входящих в предмет доказывания. Вместе с тем, эта классификация предопределяет и место информации в системе доказательств: если электронные носители первых трех видов информации будут являться, согласно ст. 81 УПК РФ, вещественными доказательствами, то носители четвертого вида информации при условии ее документированного характера будут являться иными документами, согласно ст. 84 УПК РФ.

По отношению к предмету доказывания информация на электронных носителях включает в себя фактические данные (информацию о юридически значимых фактах и обстоятельствах, имеющих значение для дела) и метаданные (информацию о признаках фактических данных, характеризующих обстоятельства их создания и модификации).

Вопросы для повторения:

1. Дать понятие конфиденциальной информации.
2. Перечислите, какая информация относится к конфиденциальной.
3. Назвать нормативно-правовую базу, регулирующую отношения с конфиденциальной информацией и информацией, относящейся к охраняемой федеральным законом.
4. Охраняемая федеральным законом тайна: понятие, виды.
5. Налоговая тайна, банковская тайна, тайна личной жизни: понятие, примеры.

Практическое задание:

Вам предложен отрывок приговора, необходимо определить, какой вид тайны нарушен обвиняемым, и указать федеральный закон, регулирующий данный вид деятельности.

1. «При хищении денежных средств со счёта потерпевшей с использованием пароля доступа к специальной программе подсудимая на своём рабочем месте в офисе Сбербанка России незаконно, в нарушение

предписаний ФЗ …, из корыстной заинтересованности, без согласия владельца использовала сведения, известные ей по службе, понимая, что неизбежно нарушит…тайну и желая этого».

2. «Иванов, действуя из корыстной заинтересованности, осознавая, что разглашение сведений, составляющих…тайну, недопустимо и является уголовно наказуемым деянием, пользуясь своим служебным положением, позволяющим получить информацию о юридических лицах, и имея доступ к базе данных, где содержатся сведения о юридических лицах, в нарушение требований ФЗ …, определяющих, что сведения о номере, о дате выдаче и об органе, выдавшем документ, удостоверяющий личность физического лица, не подлежат разглашению посторонним лицам, и требований ч. 1 ст. 102…кодекса Российской Федерации, в нарушение требований, предусмотренных ч. 2 ст. 102…кодекса Российской Федерации, определяющей, что…тайна не подлежит разглашению… органами, распечатал из электронной базы данных Единого государственного реестра юридических лиц информацию об ООО, где содержались сведения об указанных коммерческих организациях, в том числе паспортные данные учредителей, доли в уставных капиталах фирм, сведения, составляющие…тайну».

Глава 3. Характер правовой регламентации соответствующего вида информации

Процессуальный порядок собирания доказательственной информации на электронных носителях непосредственно зависит от характера правовой регламентации соответствующего вида информации, на что обращают внимание уважаемые ученые В. Б. Вехов и Ю. В. Гаврилин. С учетом работ вышеназванных авторов, а также на основании результатов содержательного анализа собственных эмпирических данных представляется возможным выделить ***следующие виды информации, содержащейся на электронных носителях***:

1) электронный документ – это 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.

Использование электронных документов при совершении преступлений рассмотрим в следующем примере.

В рамках расследования уголовного дела установлено, что из корыстных побуждений в целях личного обогащения у гражданки М. возник прямой преступный умысел, направленный на контрабанду стратегически важных ресурсов, то есть незаконное перемещение через таможенную границу Таможенного союза в рамках ЕврАзЭС стратегически важных ресурсов в крупном размере путем недостоверного декларирования – указания в таможенных декларациях на товары недостоверных сведений о производителе, сопряженного с использованием документов, содержащих недостоверные сведения о происхождении товара, при исполнении условий контрактов поставки стратегически важных ресурсов. Реализуя свой прямой преступный умысел, гражданка М. совершила контрабанду, то есть незаконное перемещение через таможенную границу Таможенного союза в рамках ЕврАзЭС лесоматериалов из Российской Федерации в Китайскую Народную Республику в крупном размере.

Перемещение товаров через таможенную границу с недостоверным декларированием, либо с использованием документов, содержащих недостоверные сведения о товарах, является незаконным перемещением товаров через таможенную границу. Лесоматериалы включены в Перечень

стратегически важных ресурсов для целей ст. 226.1 Уголовного кодекса Российской Федерации, утвержденный постановлением Правительства Российской Федерации от 13 сентября 2012 года № 923. В соответствии со ст. 6 Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи», информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Из протокола обыска следует, что проведен обыск в офисе консалтингового агентства, в ходе чего изъяты электронные документы и предметы, принадлежащие ООО[76].

Несмотря на наличие законодательной дефиниции, в литературе данное понятие рассматривается в узком и широком смыслах. Узкий подход основан на приведенном выше законодательном определении. Так, 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. Информация, сведения, данные являются терминами-синонимами».

Заслуживает внимания позиция Е. Ю. Сабитовой, которая определяет документ (в целом) как «созданный человеком материальный носитель, на котором информация отображена в виде символов и сигналов и который предназначен для ее хранения и передачи во времени и пространстве».

О. А. Городов выделил следующие признаки электронного документа:

1) наличие материального носителя информации;

2) наличие реквизитов, которые помогают идентифицировать полученные на материальный носитель сведения, а также когда имеется возможность в установлении источника происхождения данной

[76] Приговор № 1-856/2018 1-90/2019 от 6 февраля 2019 г. по делу № 1-856/2018 Октябрьский районный суд г. Улан-Удэ (Республика Бурятия).

информации, ее назначение, время документирования, а в ряде случаев имеется возможность обеспечить защиту документа от подделки;

3) подлежащая изменению форма фиксации документированной информации. Это сведения, зафиксированные на материальном носителе одного вида, которые могут одновременно быть представлены на других видах носителей без угрозы утраты своего содержания и реквизитов.

Широкий подход к понятию «электронный документ» прослеживается, например, у А. Б. Борковского, который считает, что электронный документ – это совокупность данных в памяти вычислительной системы, предназначенных для восприятия человеком с помощью соответствующих программных и аппаратных средств.

По мнению И. Н. Подволоцкого, являющегося также сторонником расширительного толкования термина «электронный документ», электронный документ – это та информация, которая может храниться, обрабатываться и передаваться с помощью как автоматизированных информационных, так и телекоммуникационных систем, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном уголовно-процессуальным законодательством, устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела, которые могут быть получены при соблюдении норм процессуального права и приобщены к уголовному делу.

С данным подходом, отраженным в приведенных позициях процитированных авторов, согласиться не представляется возможным по причине отсутствия ключевого признака электронного документа – документированного характера содержащейся в нем информации, что подробно было рассмотрено выше[77].

Электронное сообщение представляет собой информацию, которая передается (получается) пользователем информационно-телекоммуникационной сети[78]. Примером использования электронных сообщений в процессе доказывания является следующий.

---

[77] Более подробно см.: Балашова А.А. К вопросу о понятии «электронное доказательство» // Закон и право : науч. журн. Москва. 2018. № 6. С. 120–122.

78 Об информации, информационных технологиях и о защите информации: Федер. закон № 149-ФЗ : послед. ред. : принят Государственной Думой 08 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264 (дата обращения: 25.02.2022). Режим доступа: свободный.

Предварительным расследованием по уголовному делу № 1-120/2019, связанному с незаконным сбытом синтетических наркотических средств бесконтактным способом – через закладки с использованием информационно-телекоммуникационной сети Интернет, было установлено, что основной преступной деятельностью созданного преступного сообщества являлась продажа запрещенных в Российской Федерации веществ через сайт «Р.», электронные платежные системы «Qiwi», «PAYEER», «Bitcoin», «Litecoin» и сервис мгновенного обмена электронными сообщениями Telegram. Участники преступного сообщества (преступной организации) сообщали покупателям на сайте «Р.» или в электронном сообщении Telegram информацию о местонахождении наркотических средств. В процессе расследования были изъяты мобильные телефоны с установленной программой Telegram, как в ходе личного досмотра обвиняемых, так и в ходе обыска по месту жительства. В процессе осмотра мобильного телефона установлено: в памяти обнаружена программа обмена сообщениями Telegram и электронные сообщения в виде переписки между членами преступного сообщества с контактами о местонахождении и торговле наркотическими средствами[79].

В ходе расследования уголовного дела, гражданин Х. совершил хранение, перевозку в целях сбыта и сбыт поддельных банковских билетов Центрального банка Российской Федерации.

Гражданин Х., находясь в квартире, посредством информационно-телекоммуникационной сети Интернет, используя браузер Tor Browser, на интернет-сайте HYDRA, используя свой аккаунт, путем обмена электронными сообщениями заказал с целью сбыта у неустановленного лица в интернет-магазине не менее 8 заведомо поддельных банковских билетов ЦБ РФ, после чего в этот день по полученным на своем аккаунте координатам на интернет-сайте HYDRA забрал указанные поддельные банковские билеты ЦБ РФ из «закладки» – скрытого места расположения[80].

Сайт в сети Интернет – это программы, предназначенные для ЭВМ, а также информации, которая содержится в информационной системе, доступ к которой обеспечивается посредством сети Интернет по доменным

[79] Приговор Псковского городского суда от 22.08.2019 по делу № 1-120/2019.

[80] Приговор № 1-539/2020 от 15 октября 2020 г. по делу № 1-539/2020 Псковский городской суд (Псковская область).

именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети Интернет[81].

Нижеприведенный пример – подтверждение доказательственного значения информации, размещенной на сайте в сети Интернет: с целью доказывания вины обвиняемой в совершении преступления, предусмотренного ч. 1 ст. 293 УК РФ, был произведен осмотр официального портала органов власти Калужской области admoblkaluga.ru, на котором имеется ссылка: «Спортивная площадка в д. Горки Перемышльского…». Данная информация имела доказательственное значение для уголовного дела[82].

В ходе расследования еще одного уголовного дела, установлено: гражданин С., гражданин Г. и гражданин П. совершили покушение на незаконный сбыт наркотических средств, совершенный с использованием электронных и информационно-телекоммуникационных сетей (включая сеть «Интернет»), организованной группой.

Согласно протоколу осмотра предметов, на стационарном компьютере осмотрен сайт в сети Интернет. Данный протокол осмотра, в ходе которого установлено существование Интернет**,** отражены условия работы, оплата, суд признает допустимым доказательством, полученным с соблюдением требований уголовно-процессуального законодательства[83].

Страница сайта в сети Интернет (интернет-страница) представляет собой часть сайта в сети Интернет, доступ к которой осуществляется по указателю, который состоит из доменного имени и символов, определенных владельцем сайта в сети Интернет[84].

Так, в ходе расследования уголовного дела предварительным следствием уставлено, что гражданин К. посредством оператора сотовой связи «МТС», используя известные ему логин и пароль, осуществил неправомерный доступ на личную страницу гражданки Р. на сайте «ВКонтакте» ID223395140. После чего К. совершил умышленные действия по модификации компьютерной информации на личной странице гражданки Р.[85]

---

[81] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019).

[82] Приговор Козельского районного суда Калужской области от 22.08.2019 по делу № 1-3-21/2019.

[83] Приговор № 1-272/2019 от 16 июля 2019 г. по делу № 1-272/2019 Абаканский городской суд (Республика Хакасия).

[84] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019). Ст. 2.

[85] Дело № 1-123/2019 // Архив Сарапульского городского суда Удмуртской Республики.

В ходе расследования уголовного дела в г. Чита, установлено, что гражданка Д., действуя умышленно, из корыстных побуждений, в целях получения доходов от незаконного сбыта наркотических средств посредством сети Интернет, договорившись о совместном совершении преступления, вступила в предварительный сговор с неустановленным лицом, зарегистрированным в сети Интернет под неустановленным именем, на незаконный сбыт наркотических средств путем проведения закладок с использованием информационно-телекоммуникационной сети Интернет и электронной сети – электронной платежной системы QIWI в целях систематического получения доходов.

Согласно протокола осмотра предметов осмотрена страница сайта в сети Интернет с указателем, который был отправлен «privozwork» с описанием места муляжа наркотического средства в рамках проведения ОРМ «Оперативный эксперимент»[86].

Доменное имя – это обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет[87]. В этих же целях возможно использование и *сетевого адреса (IP-адрес)* – это определенный числовой идентификатор в сети передачи данных. Он определяется при оказании телематических услуг связи абонентского терминала или иных средств связи, входящих в информационную систему.

Пример доказательственного значения доменного имени для уголовного дела: обвиняемый В., обладая достаточными познаниями и имеющий практический опыт работы в глобальной информационно-коммуникационной сети Интернет, используя электронно-вычислительную машину, преодолевая защиту компьютерной информации, нарушая требования законодательства Российской Федерации, охраняющего компьютерную информацию, осуществил выход в сеть Интернет на сайт с доменным именем ….cht.sudrf.ru, принадлежащий Читинскому районному суду. При этом В., зная логин и пароль и осознавая, что пароль является конфиденциальной информацией и ему не принадлежит, а доступ к административному разделу сайта с доменным именем ….cht.sudrf.ru ему запрещен, ввел их для получения доступа к административной части сайта, получив возможность изменять и блокировать доступ к сайту. В процессе

[86] Приговор № 1-659/2017 от 27 ноября 2017 г. по делу № 1-659/2017 Центральный районный суд г. Читы (Забайкальский край).

[87] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019). Ст. 2.

расследования был произведен осмотр компьютера помощника председателя суда, в ходе которого получена информация со страницы системного журнала, содержащая записи об осуществлении соединения с сервером, случаи доступа к компьютерной информации и список событий. В результате доступа пользователя к административному разделу сайта с доменным именем ….cht.sudrf.ru проводились уничтожение и модификация информации[88].

Об использовании в преступной деятельности сети Интернет, доменных имен свидетельствует и следующий пример.

Так, гражданка С. совершила участие в преступном сообществе (преступной организации) при следующих обстоятельствах: основной преступной деятельностью созданного преступного сообщества (преступной организации) являлась продажа запрещенных в Российской Федерации синтетических наркотических средств бесконтактным способом – через закладки с использованием информационно-телекоммуникационной сети Интернет – сайта «р.», электронных платежных систем Qiwi, PAYEER, Bitcoin, Litecoin и сервиса мгновенного обмена электронными сообщениями Telegram.

После его блокировки члены преступной группы объявили о своем сайте в сети Интернет с доменным именем «р.», который в дальнейшем продолжили использовать для продажи наркотиков. Одновременно члены преступной группы продолжили создавать и запускать новые аккаунты-боты Telegram для продажи наркотиков.

Доказательствами преступной деятельности стали показания свидетеля Ф. Д. о том, что сетевой адрес включен в Единую автоматизированную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» на основании решения МВД России №8/7/10-19322 о признании информации на указанном ресурсе запрещенной к распространению на территории Российской Федерации. Возможность получить доступ к сайту, когда его доменное имя и IP-адрес включены в Единую автоматизированную информационную систему, имеется.

[88] Приговор Центрального районного суда г. Читы Забайкальского края от 29.05.2019 по делу № 1-360/2019.

Протокол осмотра предметов, в ходе которого осмотрены: карта памяти 2 Gb, в ходе осмотра которой установлено, что в ее памяти имеется файл с изображением граффити на стене с надписью доменного имени сайта «***»[89].

Системная информация – разновидность служебной информации, которая предназначена для осуществления определенных функций отдельных микропроцессорных устройств, информационных систем, информационных сетей. Таковой является, например, содержание электронных журналов регистрации событий в информационной системе. В предыдущем примере таковой являлось содержание системного журнала, содержащего записи об осуществлении соединения с сервером, случаи доступа к компьютерной информации и список событий. К системной информации относятся и *метаданные* – вспомогательные технические сведения относительно основной информации, включая: внутренние (имя, размер и формат файла); административные (автор файла, дата и время создания, изменения); описательные (связи файла, его категории).

Так, в ходе расследования уголовного дела установлено, что гражданин Б. совершил мошенничество, то есть хищение чужого имущества путем обмана и злоупотребления доверием с использованием своего служебного положения, в крупном размере.

Доказательством его вины стало заключение эксперта, составленное по результатам исследования персонального компьютера, находящегося в пользовании гражданина Б. Согласно выводам эксперта, в компьютере сохранены сведения об учетных записях Интернет в системах "iCloud" и "Game Center"; 1. iCloud. В метаданных файла имеется информация о том, что файл сохранен 16.01.2017 в 16:29 гражданином Б.[90].

В ходе расследования уголовного дела установлено, что гражданин К. в определенный период года из корыстных побуждений решил похитить путем обмана денежные средства в размере 56 % оклада по воинской должности, не положенные ему к выплате. Доказательством вины является заключение компьютерной экспертизы, в ходе проведения которой установлено, что файл под названием «Выписка из приказа», содержащий выписку из приказа руководителя, обнаруженный в ходе осмотра

[89] Приговор № 1-197/2019 1-2/2020 от 15 июля 2020 г. по делу № 1-197/2019 Псковский городской суд (Псковская область).

[90] Приговор № 1-224/2019 от 19 июля 2019 г. по делу № 1-224/2019 Верх-Исетский районный суд г. Екатеринбурга (Свердловская область).

компьютеров финансового отдела, в которой гражданину К. установлена надбавка за риски в размере 100 процентов оклада по воинской должности, содержит следующие метаданные: автор, организация, кем изменен – user, и т.д. Показания эксперта о том, что в заключении указаны метаданные электронных файлов, исходя из всемирного координированного времени (UTC)[91].

Индивидуализирующая информация включает в себя имена пользователя, пароли, коды доступа, электронную подпись, иную информацию и программы, позволяющие идентифицировать пользователя. Примером применения индивидуализирующей информации при совершении преступления является факт использования гражданином Г. неустановленного электронного устройства, обладающего доступом к телекоммуникационной сети Интернет, посредством которого он осуществил выход в сеть Интернет, где, используя VPN-технологии и программы-анонимайзеры как средства сокрытия через удаленные серверы информации о фактическом пользователе или используемом персональном электронном устройстве, через которое осуществляется выход в глобальную телекоммуникационную сеть Интернет по IP-адресам, зная логин (наименование почты) и пароль электронной почты, ввел их для получения доступа к электронному почтовому ящику указанной почты, принадлежащей легальному пользователю – ООО «Фирма «Теле-сервис», при этом осознавая, что логин и пароль ему не принадлежат, пароль является конфиденциальной информацией, а доступ к указанному электронному почтовому ящику электронной почты ему запрещен, осуществил неправомерный доступ к содержимому электронного почтового ящика электронной почты, в котором находилась охраняемая законом компьютерная информация[92].

В ходе расследования уголовного дела, установлено, что гражданин Н. в запланированное время, используя незаконно добытые имя пользователя и код доступа для осуществления онлайновых безналичных банковских операций, принадлежащие компании «Penneco Pipeline Corporation» в лице ответственного сотрудника компании – старшего вице-президента, должен был произвести несанкционированный перевод денежных средств, принадлежащих компании «Penneco Pipeline

---

[91] Приговор № 1-84/2017 от 1 сентября 2017 г. по делу № 1-84/2017 Екатеринбургский гарнизонный военный суд.

[92] Дело № 1-442/2018 // Архив Одинцовского городского суда Московской области.

Corporation», на банковский счет, получив несанкционированный доступ в систему онлайновых банковских операций банка «First Commonwealth Bank», имея цель хищения чужого имущества путем обмана, воспользовавшись незаконно добытыми именем пользователя и кодом доступа, принадлежащими компании «Penneco Pipeline Corporation», направил в банк поручение о совершении банковской операции по безналичному перечислению денежных средств[93].

Программа для ЭВМ – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата. Сюда входят и подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения[94].

Боднарук М. Ю. в своей работе, рассматривая обстоятельства, при которых происходит соответствующее нарушение порядка использования программы для ЭВМ (в частности, форма вины лицензиата, личность субъекта правонарушения, вовлеченность такого субъекта в осуществление предпринимательской деятельности), опираясь на нормы Гражданского кодекса Российской Федерации, выделяет способы использования именно программы для ЭВМ, к которым относит следующие:

– воспроизведение программного обеспечения (далее ПО), т.е. есть изготовление одного и более экземпляра ПО или его части в любой материальной форме, включая запись в память ЭВМ;

– распространение ПО путем продажи или иного отчуждения его экземпляров;

– публичный показ ПО;

– импорт экземпляров ПО в целях распространения;

– прокат экземпляра ПО, когда программа является основным объектом проката;

– модификация ПО, т.е. любые его изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой язык;

---

[93] Приговор № 1-10/2016 1-399/2015 от 14 января 2016 г. по делу № 1-10/2016 Ленинский районный суд г. Краснодара (Краснодарский край).

[94] Гражданский кодекс Российской Федерации (часть четвертая): ГК : в послед ред. : принят Гос. Думой 24 ноября 2006 года : одобрен Советом Федерации 8 декабря 2006 года // КонсультанПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 25.11.2021). Режим доступа: свободный.

– доведение ПО до всеобщего сведения таким образом, что любое лицо может получить доступ к ПО из любого места и в любое время по собственному выбору (доведение до всеобщего сведения), т.е. передача экземпляра по сети Интернет.

Таким образом, именно в лицензионном договоре должны быть названы все конкретные способы использования программы для ЭВМ лицензиатом[95].

В качестве примеров использования программ для ЭВМ в качестве доказательств, можно рассмотреть следующие:

1. В рамках расследования уголовного дела № 6747 установлено, что гражданин Д. с целью исключения материальных затрат на приобретение лицензионного программного обеспечения, вопреки воле правообладателей и без заключения с ними договоров незаконно хранил и использовал на служебном компьютере при осуществлении коммерческой деятельности по изготовлению и установке пластиковых окон и балконных конструкций один экземпляр программы для ЭВМ «ПрофОкна», исключительные права на которую принадлежали ООО «ПрофСегмент», стоимостью 514 700 рублей, что является крупным размером[96].

2. В рамках расследования уголовного дела № 1-87/2019 установлено, что гражданин С., являясь генеральным директором общества с ограниченной ответственностью, умышленно, из корыстных побуждений, незаконно использовал объекты авторского права в крупном размере, с использованием своего служебного положения. Так, гражданин С., находясь в служебном помещении, получил обязательное представление, после чего из корыстных побуждений, с целью незаконного извлечения для себя материальной выгоды, вопреки воле правообладателя, без заключения с ним договора, в нарушение ч. 1 ст. 44 Конституции Российской Федерации, в соответствии с которой интеллектуальная собственность охраняется законом; в нарушение п. 1 ст. 1229 ГК РФ, в соответствии с которым использование результата интеллектуальной деятельности без согласия правообладателя является незаконным; в нарушение п. 1 ст. 1270 ГК РФ, в соответствии с которым

---

[95] Боднарук М.Ю. Способы нарушения исключительного права правообладателя на программу для ЭВМ через призму понятия «ПИРАТСТВА» // Вестник Волжского университета им. В. Н. Татищева : науч. журн. Тольятти : Волжский университет им. В. Н. Татищева. 2021. № 2, том 1. С. 186.

[96] Приговор Красногорского районного суда Московской области от 27.02.2019 по делу № 1-41/2019.

правообладателю принадлежит исключительное право использовать произведение и разрешать использование третьим лицам программы для ЭВМ, является и хранение экземпляра программы в памяти ЭВМ. У гражданина С. возник преступный умысел, направленный на незаконное использование в крупном размере объектов авторского права, к которым в соответствии с п. 1 ст. 1259 ГК РФ относятся программы для ЭВМ. Таким образом, гражданином С. были использованы программы для ЭВМ, исключительные права на которые принадлежат фирме, на общую сумму 103 000 рублей, то есть в крупном размере[97].

База данных – это представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ)[98].

Так, в ходе расследования уголовного дела № 236 установлено, что гражданка В., имеющая в связи со своим служебным положением доступ к базе данных с конфиденциальной информацией о счетах клиентов Сбербанка России, на своем служебном компьютере, используя свои персональные данные для входа в систему, вошла в служебную программу и осуществила неправомерный перевод денежных средств[99].

Другой пример. В ходе расследования уголовного дела было установлено, что гражданка Б. совершила кражу, то есть тайное хищение чужого имущества, с банковского счета, кроме того, совершила кражу, то есть тайное хищение чужого имущества, с причинением значительного ущерба гражданину, с банковского счета, а также совершила незаконное использование сведений, составляющих банковскую тайну. Гражданка Б., используя свои логин и пароль для входа в программное обеспечение ПАО «Почта Банк», которые ей были предоставлены для работы, используя сфотографированное при помощи веб-камеры на ее рабочем месте фото клиента С., хранящееся в программном обеспечении Банка, умышленно вошла в банковскую автоматизированную систему «SIEBEL», содержащую сведения об операциях, счетах и вкладах клиентов Банка,

[97] Приговор № 1-115/2019 от 20 сентября 2019 г. по делу Сухоложский городской суд (Свердловская область).

[98] Гражданский кодекс Российской Федерации (часть четвертая).

[99] Приговор от 22.03.2019 по делу № 1-71/2019 // Архив Зеленоградского суда г. Москвы.

незаконно, с корыстной целью, умышленно оформила заявление (анкету) с персональными данными клиента С. Направила заявку для принятия Банком решения о выдаче кредита, после одобрения Банком заявки гражданка Б., используя базы данных автоматизированных систем Банка, процедуры доступа к информационным ресурсам Банка, в карточке клиента С. незаконно умышленно внесла необходимые данные для оформления потребительского кредита, указав номер банковской карты, выданной ей ранее для оформления кредитных продуктов, тем самым автоматически открыла на имя клиента С. счет[100].

Электронная подпись – определенная информация, находящаяся в электронной форме, присоединяющаяся к другой информации, которая, в свою очередь, находится также в электронной форме (подписываемой информации) или иным образом связана с такой информацией. Она используется для определения лица, подписывающего информацию[101].

Федеральный закон «Об электронной цифровой подписи» определяет, что электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Средством проверки документа в электронном виде будет наличие электронной цифровой подписи, в связи с чем документ приобретает юридический статус и имеет такую же юридическую силу, как бумажный документ с собственноручной подписью и печатью.

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

---

[100] Приговор № 1-371/2020 от 10 июля 2020 г. по делу № 1-371/2020 Братский городской суд (Иркутская область).

[101] Об электронной подписи : Федер. закон № 63-ФЗ : принят Гос. Думой 25 марта 2011 г.: одобрен Сов. Федерации 30 марта 2011 г. (ред. от 02.07.2021) // КонсультанПлюс : сайт. URL: http://www.consultant.ru/document/ cons_doc_LAW_112701/ (дата обращения: 25.08.2019). Режим доступа: свободный.

По сути, цифровая подпись является одним из средств применения криптографии, используемым в качестве подтверждения волеизъявления участников как аналог собственноручной подписи на обычном документе.

На сегодняшний день электронная цифровая подпись – это эффективное средство защиты информации от модификации, которое переносит свойства реальной подписи под документом в область электронного документооборота. Благодаря тому, что информационные технологии и законодательство не стоят на месте, в недалеком будущем в реальности уже новый виток развития электронной подписи с участием облачных вычислений.

В ходе расследования уголовного дела № 156534 установлено, что для реализации своего преступного умысла гражданин В. подписал с применением усиленной квалифицированной электронной подписи, подтвердив тем самым, якобы, подлинность и достоверность представляемых сведений, и представил в Межрайонную инспекцию Федеральной налоговой службы России посредством телекоммуникационных каналов связи налоговые декларации, содержащие заведомо ложные сведения.

Еще один интересный пример. В ходе расследования уголовного дела было установлено, что гражданка Г. совершила предоставление документа, удостоверяющего личность, для внесения в Единый государственный реестр юридических лиц сведений о подставном лице, а также сбыт электронных средств, электронных носителей информации, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств.

Установлено, что гражданка Г. в установленный период, действуя в целях реализации своего преступного умысла, после получения электронных средств – логина, пароля и SMS-сообщения с кодами, а также электронного носителя информации – банковской карты «Visa Unembossed», необходимых для распоряжения денежными средствами, находящимися на расчетных счетах ООО в ПАО, будучи надлежащим образом ознакомленной с Правилами банковского обслуживания при оказании услуги «Дистанционное открытие / сопровождение / закрытие банковского счета корпоративному клиенту», условиями использования системы ДБО «Интернет-Банк Light», а также в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и

финансированию терроризма» и Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе», согласно которым участники обязуются соблюдать конфиденциальность и секретность в отношении логина, пароля и ключа электронной подписи уполномоченного лица, не разглашать их третьим лицам, немедленно информировать банковские организации обо всех случаях компрометации ключа электронной подписи, из корыстных побуждений, за денежное вознаграждение, посредством использования открытых расчетных счетов, по ранее достигнутой договоренности, передала (сбыла) указанные электронные средства и электронные носители информации неустановленному лицу. Таким образом, гражданкой Г. был получен доступ к электронным средствам – активированным ключам электронной подписи для проверки подлинности электронной подписи, а также электронному носителю информации – банковской карте, выданной для осуществления расчетов по банковскому счету ООО в ПАО «Промсвязьбанк»[102].

Вредоносная программа – программа, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации[103].

Так, в ходе расследования уголовного дела следственным управлением УМВД России по Владимирской области было установлено, что Л. вступил в преступный сговор с неустановленным лицом, направленный на хищение денежных средств из банкоматов, расположенных на территории Владимирской области. С указанной целью Л., запустив вредоносную компьютерную программу, модифицировал компьютерную информацию банкомата, нейтрализовал средства защиты и инициировал автоматическую выгрузку денежных средств из банкомата[104].

При расследовании уголовного дела № 1-40/2020 установлено, что гражданин К. совершил использование компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации. У гражданина К. возник умысел,

---

[102] Приговор № 1-1132/2020 от 26 ноября 2020 г. по делу № 1-1132/2020 Вологодский городской суд (Вологодская область).

[103] Уголовный кодекс Российской Федерации : УК : в послед. ред. : принят Гос. Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 25.08.2021). Режим доступа: свободный.

[104] Приговор Октябрьского районного суда г. Владимира (Владимирская область) от 04.06.2019 по делу № 1-95/2019.

направленный на использование вредоносной компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации, реализуя который, гражданин К. на не установленном следствием интернет-ресурсе скопировал на свою персональную электронно-вычислительную машину файлы вредоносной компьютерной программы, предназначенной для нейтрализации средств защиты компьютерной информации. Вина гражданина К. доказана в том числе и заключением эксперта, согласно которому на оптическом диске, представленном на экспертизу, содержится файл, содержащий в себе сведения об интернет-трафике, который свидетельствует о деструктивном воздействии с IP-адреса на адрес назначения IP-адрес с использованием вредоносного программного обеспечения. Также имеется заключение эксперта, согласно которому на жестком диске WD имеется каталог, в котором имеется исполняемый файл, именующий себя. Согласно выводам эксперта, это программа для поиска в сети интернет веб-интерфейсов сетевого оборудования, с целью дальнейшего получения несанкционированного доступа к нему. Несанкционированный доступ достигается путем нейтрализации средств защиты веб-интерфейса сетевого оборудования с помощью подбора пары логин/пароль либо эксплуатации программных уязвимостей указанного оборудования. Программа предоставляет возможность пользователю нейтрализовать средства защиты компьютерной информации, то есть является вредоносной компьютерной программой[105].

Охраняемая компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации, – это определенная информация, которая включена в реестр учета значимых объектов критической информационной инфраструктуры в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

В ходе расследования уголовного дела установлено, что гражданин Л., гражданин Л.1 и гражданин О. группой лиц по предварительному сговору совершили преступление в сфере компьютерной информации.

Так, гражданин Л., действуя умышленно, незаконно, незаконным путем, имея умысел, направленный на неправомерный доступ к критической информационной инфраструктуре Российской Федерации и

[105] Приговор № 1-40/2020 от 25 ноября 2020 г. по делу Павловский районный суд (Воронежская область).

получение имущественной выгоды от неправомерного доступа к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации – АО «Восточная верфь», путем использования вредоносных программ, вступил с гражданином Л 1. и гражданином О. в преступный сговор, направленный на неправомерный доступ к компьютерной информации АО «Восточная верфь».

Гражданин Л., находясь у себя дома с помощью, гражданин Л1., находясь у себя дома в определенный период времени, с помощью ноутбука, действуя совместно, согласно достигнутой ранее преступной договоренности, используя предоставленную гражданам О. информацию о выявленных IP-адресах, номерах портов подключения, логинах и паролях доступа к ЭВМ, используя компьютерную программу получили удалённый доступ к ЭВМ АО «Восточная верфь», после чего, осуществили неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации путем ее блокирования и модификации, что повлекло причинение вреда АО «Восточная верфь» и причинение имущественного вреда указанной организации на сумму 655 034,52 рублей[106].

Итак, виды информации, содержащейся на электронных носителях, – это:

– электронный документ;

– электронное сообщение;

– сайт в сети Интернет;

– страница сайта в сети Интернет (интернет-страница);

– доменное имя;

– системная информация;

– индивидуализирующая информация;

– программа для ЭВМ;

– база данных;

– электронная подпись;

– вредоносная программа;

– охраняемая компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации.

[106] Приговор № 1-376/2019 от 25 сентября 2019 г. по делу № 1-376/2019 Первомайский районный суд г. Владивостока (Приморский край).

Каждый вид информации имеет свои особенности. Сотрудникам правоохранительных органов необходимо совершенствовать свои знания и различать виды информации, которые находятся на электронных носителях. При расследовании уголовных дел стоит руководствоваться нормативными актами, справочными материалами, а также привлекать IT-специалистов, чтобы безошибочно определять и классифицировать виды информации. Это поможет в дальнейшем при составлении процессуальных документов (допросы, постановления о привлечении в качестве обвиняемого, обвинительное заключение и т.д.).

Вопросы для повторения:

1. Дать характеристику электронному документу, раскрыть его признаки, привести примеры.
2. Что такое электронное сообщение? Привести примеры, когда электронное сообщение может быть доказательством по уголовному делу.
3. Охарактеризовать понятие «сайт сети Интернет», страница сайта в сети Интернет (интернет-страница), привести примеры доказательственного значения информации, размещенной на сайте в сети Интернет и страницы сайта в сети Интернет (интернет-страница).
4. Раскрыть понятие электронная подпись.
5. Раскрыть понятие вредоносной программы.
6. Раскрыть понятие охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, привести примеры использования данной информации в качестве доказательства.

Практические задания:

1. Подготовить презентацию на тему «Электронная подпись».
2. В суд поступила апелляционная жалоба гражданина Б. на постановление городского суда города N, которым отказано в восстановлении гражданину Б. срока на подачу апелляционной жалобы на постановление.

Направление судом электронного уведомления о принятом постановлении суда на электронный адрес гражданина Б. также было осуществлено судом с нарушением установленного законом срока, а также с несоблюдением положений п.п. 2.1.9 и 7.1 Приказа Судебного департамента при Верховном Суде РФ от 29.04.2003 № 36 «Об

утверждении Инструкции судебному судопроизводству в районном суде», поскольку заявитель на такую форму уведомления согласия не давал, и электронное уведомление не было заверено усиленной квалифицированной электронной подписью судьи.

По смыслу закона, уважительными причинами признаются те, которые препятствовали исполнению процессуального действия или исключали его своевременное совершение. Какое решение примет суд?

3. Произвести описание представленного объекта (электронного документа, сайта Интернет, страницы сайта Интернет) в виде фрагмента протокола осмотра.

Заключение

В заключение отметим, что цифровизация уголовного процесса должна проводиться одновременно с назревшими структурными новациями уголовного судопроизводства.

Отправной точкой цифровизации уголовного судопроизводства должны стать отношения, стоящие в самом начале процесса уголовного преследования.

Цифровизация уголовного процесса позволит исключить обязательное присутствие человека и направить заявление в правоохранительные органы, в суд с помощью современных средств коммуникации.

В этом случае первым документом в цифровом формате уголовного дела должны стать:

– заявление о преступлении;

– явка с повинной;

– постановление прокурора о направлении соответствующих материалов в органы предварительного расследования для решения вопроса об уголовном преследовании;

– или сообщения о совершенном либо готовящемся преступлении, полученные из иных источников.

Только система, всесторонний подход к цифровизации уголовного судопроизводства сможет создать реальные возможности его качественного продвижения.

При расследовании уголовного дела необходимо помнить, что процессуальный порядок собирания доказательственной информации на электронных носителях находится в прямой зависимости от вида самой информации и ее правовой природы.

Необходимо помнить, что по своему содержанию информация с ограниченным доступом объединяет всю совокупность сведений, составляющих как тайную, так и конфиденциальную информацию, нуждается в защите на законодательном уровне и подлежит охране государством.

Согласно действующему законодательству, к информации ограниченного доступа также относится информация, которая не подлежит обнародованию и распространению в средствах массовой информации.

Классификация доказательственной информации на электронных носителях играет важную роль в следственной и судебной практике. Пользование классификацией, то есть ее правильное применение в этой области существенно упростят работу сотрудников полиции и судей.

Процессуальный порядок собирания информации на электронных носителях также требует определенных знаний. Правильное изъятие такой информации будет оформлено как доказательство по уголовному делу.

Рекомендуемая литература

Международные документы и нормативные правовые акты зарубежных государств

1. Конвенция о защите прав человека и основных свобод: заключена в г. Риме 04.11.1950 (с изм. от 13.05.2004) (вместе с «Протоколом [№ 1]» (Подписан в г. Париже 20.03.1952), «Протоколом № 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом № 7» (Подписан в г. Страсбурге 22.11.1984)) КонсультантПлюс : официальный сайт. URL: http://www.consultant.ru (дата обращения: 14.07.2021). Режим доступа: для зарегистрир. пользователей.

2. Хартия Европейского Союза об основных правах (Страсбург, 12 декабря 2007 г.) (2016/C 202/02) // Гарант : официальный сайт. URL: https://www.garant.ru (дата обращения: 14.07.2021). Режим доступа: свободный.

Нормативные правовые акты Российской Федерации

3. Российская Федерация. Законы. Гражданский кодекс Российской Федерации : ГК : в послед ред. : принят Гос. Думой 24 ноября 2006 года : одобрен Советом Федерации 8 декабря 2006 года // КонсультанПлюс : сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 25.11.2021). – Режим доступа: свободный.

4. Российская Федерация. Законы. Налоговый кодекс Российской Федерации : НК : в послед ред. : принят Государственной Думой 16 июля 1998 года : одобрен Советом Федерации 17 июля 1998 года (ред. от 26.03.2020; с изм. и доп., вступ. в силу с 01.04.2020)] // КонсультанПлюс : сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_19671/ (дата обращения: 25.11.2021). – Режим доступа: свободный.

5. Российская Федерация. Законы. Уголовный кодекс Российской Федерации: УК : в ред. от 01.07.2021 : принят Гос. Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года // КонсультанПлюс : сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 25.08.2021). – Режим доступа: свободный.

6. Российская Федерация. Законы. Об основах охраны здоровья граждан в Российской Федерации : Федеральный закон № 323-ФЗ : принят Государственной Думой 1 ноября 2011 года : одобрен Советом Федерации 9 ноября 2011 года // КонсультанПлюс : сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 21.02.2022). – Режим доступа: свободный.

7. Российская Федерация. Законы. Об электронной подписи : Федеральный закон № 63-ФЗ : послед. ред. : принят Государственной Думой 25 марта 2011 года : одобрен Советом Федерации 30 марта 2011

года // КонсультанПлюс : сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

8. Российская Федерация. Законы. Об официальном статистическом учете и системе государственной статистики в Российской Федерации : Федеральный закон № 282-ФЗ : послед. ред. : принят Государственной Думой 9 ноября 2007 года : одобрен Советом Федерации 16 ноября 2007 года // КонсультантПлюс: официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_72844/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

9. Российская Федерация. Законы. О персональных данных : Федеральный закон № 152-ФЗ : послед. ред. : принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года // КосультантПлюс: официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_law_61801/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

10. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : послед. ред. : принят Государственной Думой 08 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264 (дата обращения: 25.02.2022). – Режим доступа: свободный.

11. Российская Федерация. Законы. О кредитных историях : Федеральный закон № 218-ФЗ : послед ред. : принят Государственной Думой 22 декабря 2004 года : одобрен Советом Федерации 24 декабря 2004 года // КонсультантПлюс: официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_51043/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

12. Российская Федерация. Законы. О рыболовстве и сохранении водных биологических ресурсов : Федеральный закон № 166-ФЗ : послед. ред. : принят Государственной Думой 26 ноября 2004 года : одобрен Советом Федерации 8 декабря 2004 года // Официальный интернет-портал правовой информации. – URL: http://fsgzr.ru/DOC/np/federalnii-zakon-rf-ot-20.12.2004--166-fz.pdf (дата обращения: 15.01.2022). – Режим доступа: свободный.

13. Российская Федерация. Законы. О коммерческой тайне : Федеральный закон № 98-ФЗ : послед. ред. : принят Государственной Думой 9 июля 2004 года : одобрен Советом Федерации 15 июля 2004 года // КонсультантПлюс: официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

14. Российская Федерация. Законы. О связи : Федеральный закон № 126-ФЗ : послед ред. : принят Государственной Думой 18 июня 2003 года : одобрен Советом Федерации 25 июня 2003 года // КонсультантПлюс: официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

15. Российская Федерация. Законы. Об адвокатской деятельности и адвокатуре в Российской Федерации : Федеральный закон № 63-ФЗ : послед. ред. : принят Государственной Думой 26 апреля 2002 года : одобрен Советом Федерации 15 мая 2002 года // КонсультантПлюс: официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_36945/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

16. Российская Федерация. Законы. Об обязательном страховании гражданской ответственности владельцев транспортных средств : Федеральный закон № 40-ФЗ : послед. ред. : принят Государственной Думой 3 апреля 2002 года : одобрен Советом Федерации 10 апреля 2002 года // КонсультантПлюс: официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_36528/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

17. Российская Федерация. Законы. О гидрометеорологической службе : Федеральный закон от 19 июля 1998 г. № 113-ФЗ : послед. ред. // КонсультантПлюс : официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_19456/ (дата обращения: 25.02.2022). – Режим доступа: для зарегистрир. пользователей.

18. Российская Федерация. Законы. Об информации, информатизации и защите информации : Федеральный закон № 24-ФЗ (утратил силу) : послед. ред. : принят Государственной Думой 25 января 1995 года // КонсультантПлюс : официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_5887/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

19. Российская Федерация. Законы. О государственной тайне : Закон РФ от 21.07.1993 № 5485-1 : послед. ред. // КонсультантПлюс : официальный сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_2481/ (дата обращения: 25.02.2022). – Режим доступа: свободный.

20. Основы законодательства Российской Федерации о нотариате: утв. ВС РФ 11.02.1993 № 4462-1 // Государственная система правовой информации: официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102021541 (дата обращения: 15.01.2022). – Режим доступа: свободный.

21. Российская Федерация. Законы. О средствах массовой информации : Закон РФ от 27.12.1991 года № 2124-1 // Ведомости Съезда

народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 7. Ст. 300.

22. Российская Федерация. Законы. О банках и банковской деятельности: Закон РФ от 02 декабря 1990 года № 395-1 // Ведомости съезда народных депутатов РСФСР. 1990. № 27. Ст. 357.

Судебная практика

23. Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации : Определение Конституционного Суда РФ от 28.06.2012 № 1253-О // Гарант : офиц. сайт. – URL: https://base.garant.ru/70205530/ (дата обращения: 15.01.2022). – Режим доступа: свободный.

24. Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи» : Определение Конституционного Суда РФ от 02.10.2003 № 345-О // КонсультантПлюс : офиц. сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_45175/ (дата обращения: 15.01.2022). – Режим доступа: свободный.

Специальная литература

25. Андреева, О. И., Зайцев, О. А. Правовое регулирование уголовно-процессуальных отношений в цифровую эпоху / О. И. Андреева, О. А. Зайцев // Вестник Томского государственного университета : науч. журн. – Томск, 2020. – № 455. – С. 192

26. Андриенко, Ю. А. Отдельные аспекты использования информационных технологий и работы с электронными носителями информации в доказывании по уголовным делам / Ю. А. Андриенко // Вестник Сибирского юридического института МВД России : науч.-практич. журн. – Красноярск : СибЮИ МВД России, 2018. –№ 3 (32). С. 95–105.

27. Балашова, А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. … канд. юрид. наук / А. А. Балашова. – Москва, 2020. С. 5.

28. Балашова, А. А. К вопросу о понятии «электронное доказательство» / А. А. Балашова // Закон и право : науч. журн. – Москва, 2018. – № 6. – С. 120–122.

29. Баринов, С. В. Некоторые особенности преступных нарушений тайны переписки и иных сообщений, совершаемых в киберпространстве / С. В. Баринов // Сибирские уголовно-процессуальные и криминалистические чтения : науч. журн. – Иркутск : Байкальский государственный университет, 2016. – Вып. № 2. – С. 8.

30. Берг, А. И. Информация и управление / А. И. Берг, Ю.И. Черняк. – М., 1966. – 64 с.

31. Борковский, А. Б. Англо-русский словарь по программированию и информатике (с толкованиями) : ок. 6000 терминов. – М., 1992. – С. 95.

32. Вершинин, А. П. Электронный документ: правовая форма и доказательство в суде / А. П. Вершинин. – М., 2000. – С. 40–41.

33. Вехов, В. Б. Электронные доказательства: проблемы теории и практики / В. Б. Вехов // Правопорядок: история, теория, практика : науч.-практич. журнал. – Челябинск, 2016. – № 4 (11). – С. 46–50.

34. Вилкова, Т. Ю., Масленникова, Л. Н. Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов – к электронному уголовному делу / Т. Ю. Вилкова, Л. Н. Масленникова // Вестник Пермского университета. Юридические науки : науч. журнал. – Пермь : Пермский государственный национальный исследовательский университет, 2019. – Вып. 46. – С. 736.

35. Гаврилин, Ю. В. Электронные носители информации в уголовном судопроизводстве / Ю. В. Гаврилин // Труды Академии Управления МВД России : науч.-практич. журнал. – Москва : Академия управления МВД России, 2017. –№ 4. – С. 45.

36. Городов, О. А. Основы информационного права России / О. А. Городов. – СПб : Юрид. центр Пресс, 2003. – С. 45.

37. Головко, Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? / Л. В. Головко // Вестник экономической безопасности : науч. журнал. – Москва : Московский университет МВД России имени В. Я. Кикотя, 2019. – № 1. – С. 17–21.

38. Горошко, И. В., Лебедев, В. Н. Правовое регулирование передачи служебной информации ограниченного распространения в федеральных органах исполнительной власти / И. В. Горошко, В. Н. Лебедев // Юридическая наука и правоохранительная практика : науч.-практич. журнал. – Тюмень : Тюменский институт повышения квалификации сотрудников МВД России, 2020. – № 9 (53). – С. 86.

39. Грачев, С. А. Охраняемая законом тайна в уголовном судопроизводстве: коллизии теории и практики / С. А. Грачев // Юридическая наука и правоохранительная практика : науч.-практич. журнал. – Тюмень : Тюменский институт повышения квалификации сотрудников МВД России, 2020. – № 1 (51). – С. 76.

40. Григорьев, В. Н. Тенденции и проблемы развития законодательства, в области информационных технологий, регулирующих уголовное судопроизводство / В. Н. Григорьев // Академическая мысль : науч. журнал. – Москва : Академия управления МВД России, 2019. – № 3 (8). С. 58.

41. Данилова, Л. Н., Основные подходы к пониманию цифровизации и цифровых ценностей / Л. Н. Данилова, Т. В. Ледовская, Н. Э. Солынин,

А.М. Ходырев // Вестник Костромского государственного университета : науч. журнал. – Кострома : Костромской государственный университет, 2020. – № 2. – С. 8.

42. Зайцев, О. А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства / О. А. Зайцев // Журнал зарубежного законодательства и сравнительного правоведения : науч. журнал. – Москва : Норма, 2019. – № 4. – С. 54.

43. Зигура, Н. А. Компьютерная информация как вид доказательств в уголовном процессе России : дис. … канд. юрид. наук. / Н. А. Зигура. – Челябинск, 2010. – С. 86.

44. Илюшенко, М. П., Документоведение. Документ и системы документации : учебное пособие / М. П. Илюшенко, Я. З. Лившиц, Т. В. Кузнецова; под ред. Я. З. Лившиц. – Москва, 1977. – 88 с.

45. Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учебное пособие / под ред. Ю. В. Гаврилина, А. В. Победкина. – Москва, 2021. – С. 10.

46. Карлов, А. Л. Процессуальная фиксация интернет-переписки в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота наркотиков / А. Л. Карлов // Вестник Сибирского юридического института ФСКН России : науч. журнал. – Красноярск : СибЮИ МВД России, 2016. – № 4. – С. 111–117.

47. Ланцман, Р. М. Использование возможностей кибернетики в криминалистической экспертизе и некоторые проблемы уголовно-судебного доказывания : автореф. дис. … д-ра юрид. наук / Р. М. Ланцман. – М., 1970. – С. 18.

48. Марковичева, Е. В. Цифровая трансформация российского уголовного судопроизводства / Е. В. Марковичева // Правосудие/Justice : науч. журнал. – Москва : Российский государственный университет правосудия, 2020. – Т. 2, № 3. – С. 91.

49. Масленникова, Л. Н. К вопросу о первых результатах реализации научного проекта № 18-29-16018 «Концепция построения уголовного судопроизводства…, обеспечивающего доступ к правосудию в условиях развития цифровых технологий» / Л. Н. Масленникова // Lex Russica (Русский закон) : науч. юрид. журн. Москва : Московский государственный юридический университет им. О. Е. Кутафина, 2020. – Т. 73. – № 1. – С. 74.

50. Медведева, М. О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития : автореф. дис. ... канд. юрид. наук / М. О. Медведева. – Москва : Московский университет МВД России имени В. Я. Кикотя, 2018. – 29 с.

51. Минбалеев, А. В. Право на информацию: природа и особенности развития в современном мире / А. В. Минбалеев // Вопросы управления : науч.-информац. журнал. – Екатеринбург : Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, 2014. – № 4 (29). – С. 203–207.

52. Никулина, Т. В., Стариченко, Е. Б. Информатизация и цифровизация образования: понятия, технологии, управление / Т. В. Никулина, Е. Б. Стариченко // Педагогическое образование в России : международ. науч.-исслед. журнал. – Екатеринбург : Уральский государственный педагогический университет, 2018. – № 8. – С. 107–113.

53. Новолодский, Ю. М. Цифровизация уголовного судопроизводства / Ю. М. Новолодский // Федеральная палата Адвокатов Российской Федерации : сайт. – URL: https://fparf.ru/polemic/opinions/tsifrovizatsiya-ugolovnogo-sudoproizvodstva. Дата публикации: 05.05.2020. Режим доступа: свободный.

54. Панфилов, И. П. Теория электрической связи / И. П. Панфилов, В. Е. Дырда. – М.: Радио и связь, 1991. – 344 с.

55. Победкин, А. В. Этико-аксиологические риски моды на цифровизацию для уголовного судопроизводства (об ошибочности технологического подхода к уголовному процессу) / А. В. Победкин // Вестник Московского университета МВД России : науч. журнал. – Москва : Московский университет МВД России имени В. Я. Кикотя, 2020. – № 3. – С. 51.

56. Подволоцкий, И. Н. Правовые и криминалистические аспекты понятия «документ» / И. Н. Подволоцкий // «Черные дыры» в российском законодательстве : науч.-практич. юрид. журнал. – Москва, 2003. – № 2. – С. 125.

57. Сабитова, Е. Ю. Документы как признак преступлений в сфере экономики : автореф. дис. … канд. юрид. наук / Сабитова Е. Ю. – Челябинск, 2003. – С. 14.

58. Смолькова, И. В. Тайна: понятие, виды, правовая защита. Юридический терминологический словарь-комментарий / И. В. Смолькова. – М. : Луч, 1998. – С. 36–37.

59. Терехов, М. Ю. Получение дознавателями и следователями органов внутренних дел сведений, составляющих государственную или иную охраняемую федеральным законом тайну: особенности уголовно-процессуальной формы : автореф. … дис. канд. юрид. наук / М. Ю. Терехов. – М., 2010. – 32 с.

60. Троян, Н. А. Правовая информация как условие трансформации информационного общества в эпоху цифровизации / Н. А. Троян // Право и государство: теория и практика : науч. журнал. – Королёв, 2020. – № 10 (190). – С. 134.

61. Трусов, А. И. Судебное доказывание в свете идей кибернетики / А. И. Трусов // Вопросы кибернетики и право : сб. статей. – М.: Наука, 1967. – С. 20.

62. Фомичёва, Т. В., Катаева, В. И. Ценности россиян в контексте цифровизации российской экономики / Т. В. Фомичёва, В. И. Катаева // Уровень жизни населения регионов России : науч. журнал. – Москва : Федеральный научно-исследовательский социологический центр РАН, 2019. – № 2. – С. 80–84.

63. Хисматуллин, И. Г. Проблемные вопросы допустимости электронных доказательств в уголовном процессе России / И. Г. Хисматуллин // Тенденции развития науки и образования : науч. журнал. – Самара, 2020. – № 65-2. – С. 136–139.

64. Хомякова, С. С. Трансформация и закрепление термина «цифровизация» на законодательном уровне / С. С. Хомякова // Молодой ученый : науч. журнал. – Казань, 2019. – № 41 (279). – Электрон. версия. – URL: https://moluch.ru/archive/279/62867. – Дата публикации: 11.10.2019. – Режим доступа: свободный.

65. Чурикова, А. Ю. Проблемы цифровизации Российского уголовного процесса / А. Ю. Чурикова // Вестник Саратовской государственной юридической академии : науч. журнал. – Саратов : Саратовская государственная юридическая академия, 2021. – № 6 (143). – С. 212.

66. Шелегов, Ю. В., Шелегов, В. Г. К вопросу классификации электронных (цифровых) доказательств / Ю. В. Шелегов, В. Г. Шелегов // Сборник материалов XXIV международ. науч.-практич. конф. «Деятельность правоохранительных органов в современных условиях». – Иркутск : Восточно-Сибирский институт МВД России, 2019. – С. 64–68.

67. Шурухнов, Н. Г., Шагара, Г. В. Процессуальные действия на технических каналах связи как средства, законно ограничивающие конституционное право на тайну телефонных переговоров / Н. Г. Шурухнов, Г. В. Шагара // Человек: преступление и наказание : науч. журнал. – Рязань : Академия права и управления ФСИН, 2014. – № 1. – С. 84–86.

68. Щадная, М. А., Крючков, М. Д. Конфиденциальная информация: понятие, виды и уровень / М. А. Щадная, М. Д. Крючков // Евразийский Союз Ученых (ЕСУ) : науч. международ. журнал. – СПб, 2015. – № 3 (12).

69. Яковлев, А. Н. Особенности использования в расследовании преступлений компьютерной информации, похожей на тайну / А. Н. Яковлев // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений : науч. журнал. – Воронеж : Воронежский иститут МВД России, 2016. – № 1. – С. 5–11.

70. Яковлев А.Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств «Электронная почта» / А. Н. Яковлев // Вестник Воронежского института МВД России : науч.-практич. журн. – Воронеж : Воронежский институт МВД России, 2014. – № 4. – С. 42–48.

Учебное издание

Балашова Анна Александровна

ПРАВОВАЯ ПРИРОДА ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ

Учебное пособие

Редактор
Л. Ю. Ковальская

Подписано в печать 26.08.2022 . Формат 60 х 84/16
Усл. печ. л. 5,0 Тираж 50 экз. Заказ № 66.

Восточно-Сибирский институт МВД России,
г. Иркутск, ул. Лермонтова, 110.
Отпечатано в НИиРИО Восточно-Сибирского института МВД России,
г. Иркутск, ул. Лермонтова, 110.