ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ О.Е. КУТАФИНА (МГЮА)»

На правах рукописи

ПЛАТОНОВ ВАЛЕНТИН ВАСИЛЬЕВИЧ

ТЕОРЕТИКО-ПРАВОВАЯ МОДЕЛЬ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Специальность 5.1.4. Уголовно-правовые науки

Диссертация
на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук,
профессор
Малышева Ольга Анатольевна

Москва – 2026

ОГЛАВЛЕНИЕ

Введение…… 4

Глава 1. Теоретико-правовые основы электронных доказательств в уголовном судопроизводстве

§ 1.1. Электронные доказательства в уголовном судопроизводстве: сущность, отличительные свойства, генезис формирования……... 20

§ 1.2. Критерии допустимости электронного доказательства в уголовном судопроизводстве ……. 40

§ 1.3. Зарубежный опыт использования электронных доказательств в уголовном судопроизводстве и перспективы его заимствования ……. 73

Глава 2. Обеспечение юридической силы электронных доказательств в ходе предварительного расследования

§ 2.1. Собирание электронных доказательств субъектом расследования: правовое регулирование, особенности процессуального порядка …… 103

§ 2.2. Особенности проверки и оценки электронных доказательств в ходе предварительного расследования……. 133

Глава 3. Осуществление судом проверки и оценки электронных доказательств по уголовным делам …….. 154

Заключение……. 183

Список использованных источников……. 185

Приложение № 1. Проект Федерального закона «О внесении изменений и дополнений в Уголовно-процессуальный кодекс Российской Федерации»…… 218

Приложение № 2. Результаты изучения мнения должностных лиц органов предварительного расследования по проблемам использования электронных доказательств в уголовном судопроизводстве……. 232

Приложение № 3. Результаты изучения мнения адвокатов-защитников по проблемам использования электронных доказательств в уголовном судопроизводстве……. 242

Приложение № 4. Действия суда при наличии рисков признания электронных доказательств недопустимыми……..…….. 251

Приложение № 5 Методические рекомендации по порядку закрепления следователем, дознавателем электронных доказательств в ходе предварительного расследования…… 253

Введение

Актуальность темы диссертационного исследования. Прогресс науки и техники, появление многочисленных современных технических средств и способов передачи, фиксации, анализа информации затронули практически все сферы жизнедеятельности современного государства, в том числе уголовное судопроизводство. При производстве по уголовному делу допустимым стало дистанционное производство допроса, очной ставки, участие в судебных заседаниях. Развитие информационных технологий способствовало появлению как новых видов общественно опасных деяний (мошенничество с использованием электронных средств платежей, неправомерный доступ к компьютерной информации и др.), так и изменению места совершения преступлений (с традиционного (в материальном мире) на электронный формат (в виртуальную среду)) при вовлечении несовершеннолетних в совершение преступлений, осуществлении публичных призывов к осуществлению террористической деятельности и др. По многим категориям уголовных дел без обращения следователя, дознавателя, суда к электронным сведениям (электронная переписка, данные от операторов связи и сервисов о транзакциях, геолокации электронного устройства и др.) установление обстоятельств, подлежащих доказыванию, либо существенно затруднено, либо вовсе невозможно.

Следствием указанных процессов выступил устойчивый рост электронных данных, обуславливающий повышение значимости процессуальных правил их обнаружения, получения, закрепления, обеспечения сохранности, проверки при придании им доказательственного значения в уголовном судопроизводстве. Кроме того, особенность цифровой среды – нематериальный характер существования в ней объектов усложняет установление источника электронных данных, усиливает риски незаконного вмешательства в сферу охраняемых Конституцией Российской Федерации прав, свобод, законных интересов личности, организаций

(неприкосновенность частной жизни, тайна персональных данных, тайна переписки и др.). Между тем, Верховный Суд Российской Федерации[1] не исключает возможность использования электронной переписки в доказывании по уголовным делам. Правовой позицией Конституционного Суда Российской Федерации[2] не только допускается установление обстоятельств совершенного преступления посредством электронных доказательств, но и уточняется порядок изъятия электронного носителя информации.

Несмотря на возрастающую роль электронных доказательств в современном уголовном судопроизводстве, процесс уголовно-процессуального доказывания имеющих значение для уголовного дела обстоятельств с использованием указанных доказательств сопровождается рядом проблем правоприменительного характера, снижающих эффективность уголовного процесса: неполная и неоднообразная фиксация в уголовном процессе электронной переписки, файлов, аудио- и видеозаписи, извлеченных из приложений мобильных устройств сведений, наличие нередких фактов видоизменения, исчезновения электронных данных, являющихся часто ключевым носителем доказательственной информации по уголовным делам, нивелирование стандартов защиты от незаконного уголовного преследования и обвинения, снижение судебной перспективы уголовного дела, доказательственная база по которому формировалась с использованием электронных доказательств, и др.

Указанное обуславливает необходимость научно-практического обоснования нормативного закрепления в УПК РФ понятия «электронное доказательство», исследования отличительных свойств электронных уголовно-процессуальных доказательств, конкретизации процессуального порядка собирания, закрепления электронных данных в целях доказывания по уголовного делу, выявления

---

[1] Апелляционное определение Судебная коллегия по уголовным делам Верховного Суда РФ от 01 августа 2019 года по делу № 67-АПУ19-8 // СПС «КонсультантПлюс» (дата обращения: 12.04.2025).

[2] Определение Конституционного Суда РФ от 26 января 2017 года № 204-0 «Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 03.11.2025).

особенностей проверки и оценки электронных доказательств субъектом расследования, определения механизма обеспечения юридической силы электронных доказательств в ходе судебного производства по уголовным делам.

Приведенные обстоятельства подтверждают актуальность выбранной темы исследования.

Степень научной разработки темы диссертационного исследования. Теоретико-правовые основы понятия, видов электронных доказательств в уголовном судопроизводстве содержатся в научных трудах В. Б. Вехова, С. В. Власовой, В. Н. Григорьева, Ю. В. Гаврилина, Б. Я. Гаврилова, О. А. Зайцева, С. В. Зуева, Н. М. Кипнис, С. И. Кувычкова, П. Г. Марфицина, А. В. Победкина, С. Б. Россинского, Г. С. Русман, Т. К. Рябининой, А. Ю. Смолина, О. В. Химичевой, А. Ю. Черданцева и других ученых.

Проблемы использования электронных (цифровых) данных в уголовно-процессуальном доказывании раскрывались в научных работах Л. А. Воскобитовой, Л. В. Головко, посвященных цифровизации уголовного процесса, В. А. Семенцова, О. А. Малышевой, касающихся трансформации досудебного производства.

Правовой институт допустимости электронных доказательств являлся предметом исследований М. И. Воронина, Л. Н. Масленниковой, Н. М. Кипниса, определивших неоптимальность его правового регулирования УПК РФ. Гарантиям надежности электронной информации (идея «цепочки законных владений/цепочки обращения» электронных объектов) посвящены публикации А. С. Александрова. Сравнительно-правовое исследование (на примере США) использования электронных доказательств в уголовном процессе во взаимосвязи с механизмом защиты прав личности при получении электронной информации провел Р. И. Оконенко.

Вопросы проверки и обеспечения достоверности цифровых материалов в досудебном производстве в плоскости экспертологии, аутентичности аудиозаписей и иных цифровых объектов раскрывались Е. И. Галяшиной, Е. Р. Россинской, Г. П. Шамаевым и другими учеными.

Отдельные вопросы по изучаемой проблеме исследованы в докторской диссертации П. С. Пастухова «Модернизация уголовно-процессуального доказывания в условиях информационного общества», 2015 г., кандидатских диссертациях: Н. А. Зигуры «Компьютерная информация как вид доказательств в уголовном процессе России», 2010 г., Д. В. Овсянникова «Копирование электронной информации как средство уголовно-процессуального доказывания», 2015 г., С. И. Кувычкова «Использование в доказывании по уголовным делам информации, представленной в электронном виде», 2016 г., А. А. Балашовой «Электронные носители информации и их использование в уголовно-процессуальном доказывании», 2020 г., А. А. Количенко «Проблемы проверки и оценки электронных доказательств в современном уголовном процессе», 2024 г., М. Б. Набатова «Реализация права на защиту в условиях применения цифровых доказательств», 2024 г., В. Е. Смирнова «Гарантии прав личности в уголовном судопроизводстве в условиях цифровизации», 2025 г.

Результаты научных исследований указанных и других ученых имеют важное значение для теории и практики уголовного процесса. Однако в них отсутствует раскрытие комплексного и системного уголовно-процессуального обращения с электронными данными в целях уголовно-процессуального доказывания в условиях современного правового регулирования, не представлена оптимальная система критериев допустимости электронных уголовно-процессуальных доказательств, учитывающая особые свойства указанных доказательств и обеспечивающая принятие по уголовному делу законного и обоснованного итогового процессуального решения. В представленных научных работах акцент делается на техническую составляющую обращения с электронными данными, на перспективу использования их в уголовно-процессуальном доказывании. Без внимания ученых остались особенности процессуальной формы собирания следователем, дознавателем электронных доказательств, способы нивелирования факторов, препятствующих всесторонней и полной проверке указанных доказательств, правила их надлежащей оценки судом, пределы ограничения конституционных прав личности в ходе

установления фактических обстоятельств с использованием электронных доказательств.

Объектом диссертационного исследования выступают уголовно-процессуальные правоотношения, возникающие в связи с доказыванием в уголовном судопроизводстве в условиях цифровизации общественных отношений.

Предмет диссертационного исследования образуют теоретические представления об электронных доказательствах в уголовном судопроизводстве, правовые нормы, регулирующие процессуальный порядок использования субъектом расследования и судом электронных доказательств в доказывании по уголовному делу, правоприменительная практика в обозначенном направлении.

Цель диссертационного исследования – разработка теоретических положений использования электронных доказательств в уголовном судопроизводстве, а также обоснование предложений по совершенствованию уголовно-процессуального законодательства и правоприменения в обозначенной сфере.

Для достижения указанной цели поставлены следующие **задачи**:

– конкретизировать понятие, отличительные свойства электронных доказательств в уголовном судопроизводстве;

– выделить специальные критерии допустимости электронного доказательства в уголовном процессе;

– на основе сравнительно-правового анализа использования электронных доказательств в доказывании по уголовным делам определить направления заимствования положительного опыта;

– уточнить процессуальный порядок собирания и закрепления субъектом расследования электронных сведений, обеспечивающий их доказательственное значение;

– определить специфику проверки и оценки электронных доказательств в ходе предварительного расследования;

– конкретизировать порядок придания судом юридической силы электронным доказательствам в ходе рассмотрения уголовного дела по существу.

Степень достоверности результатов научного исследования обеспечивается системным характером научного исследования, его базированием на действующем законодательстве, использованием различных научных методов. Достоверность результатов диссертационного исследования также определяется обобщением мнений респондентов – 237 должностных лиц органов предварительного расследования системы МВД России, СК России и 150 адвокатов-защитников по уголовным делам по проблемам, исследуемым в диссертации, материалами судебной практики, размещенными на официальных сайтах судов общей юрисдикции, правовыми позициями Конституционного Суда Российской Федерации и Верховного Суда Российской Федерации о допустимости и порядке использования электронных доказательств в уголовном судопроизводстве.

Результаты диссертационного исследования основаны на научных позициях ученых по общим вопросам уголовного судопроизводства, а также по отдельным вопросам использования электронных доказательств в уголовном судопроизводстве с обоснованием авторской позиции по таким дискуссионным научным положениям, как: содержание понятия «электронное доказательство», конкретизация критериев допустимости электронных доказательств, необходимость правовой регламентации случаев обязательного участия специалиста в уголовном судопроизводстве, легализация процессуального порядка обеспечения сохранности электронных данных в ходе предварительного расследования и другие.

Методология и методы исследования. Основу методологии научного исследования составила материалистическая диалектика. Методология диссертации базируется на применении общенаучных (анализ, синтез, индукция, дедукция, наблюдение, статистический, герменевтический, междисциплинарный методы и др.), а также частнонаучных методов познания (сравнительно-правовой, формально-юридический и др.).

Анализ применялся при выделении структурных элементов теоретико-правовой модели электронных доказательств (понятие, свойства, виды источников

электронных доказательств, критерии допустимости, процедуры собирания и проверки); исследовании процесса обращения с электронными доказательствами (обнаружение, получение доступа, закрепление, обеспечение целостности, хранение).

Герменевтический метод использовался при интерпретации норм УПК РФ и смежного законодательства для уточнения процессуальной формы получения электронных данных, необходимых случаев осуществления судебного контроля, выявления смысла правовых позиций Конституционного Суда Российской Федерации о пределах вмешательства в тайну связи, частную жизнь, Верховного Суда Российской Федерации – относительно условий легализации электронной переписки в целях уголовно-процессуального доказывания.

Формально-юридический метод был применен при подготовке проекта федерального закона по совершенствованию положений УПК РФ, статистический метод был полезен при обобщении результатов анкетирования респондентов по исследованным в диссертации проблемам. Сравнительно-правовой метод использовался в ходе изучения зарубежного опыта использования электронных доказательств в уголовном судопроизводстве.

Теоретическую основу исследования составили труды ученых в области уголовно-процессуального права: А. С. Александрова, А. А. Балашовой, Р. С. Белкина, В. Б. Вехова, М. И. Воронина, Л. А. Воскобитовой, Л. В. Головко, О. Г. Григорьева, А. И. Зазулина, Н. А. Зигуры, С. В. Зуева, Н. М. Кипнис, П. А. Лупинской, О. А. Малышевой, Л. Н. Масленниковой, Р. И. Оконенко, П. С. Пастухова, Г. С. Русман, Т. К. Рябининой, О. В. Химичевой, С. А. Шейфера и других авторов. При подготовке диссертационного исследования автор также обращался к трудам ученых в области информационного, международного права, имеющим отношение к проблемам использования электронных доказательств в уголовном судопроизводстве.

Нормативную основу исследования составили международные правовые акты, Конституция Российской Федерации, уголовно-процессуальное законодательство Российской Федерации и ряда зарубежных государств,

касающееся вопросов использования электронных доказательств в уголовном судопроизводстве.

Эмпирическую основу исследования составили:

1) материалы судебной практики за 2020–2026 г. г. по исследуемым в диссертации вопросам, размещенные на официальных сайтах судов общей юрисдикции;

2) правовые позиции Конституционного Суда Российской Федерации и Верховного Суда Российской Федерации о допустимости использования электронных доказательств в уголовном судопроизводстве, пределах ограничения конституционных прав личности;

3) результаты изучения в 2022–2025 г. г. мнений по исследуемым проблемам 237 должностных лиц органов предварительного расследования системы МВД России, СК России в Республиках Бурятия, Саха (Якутия), Тыва, Камчатском, Краснодарском, Красноярском, Пермском, Приморском, Ставропольском, Хабаровском краях, г. Москва, Амурской, Владимирской, Волгоградской, Вологодской, Воронежской, Иркутской, Кемеровской, Кировской, Курской, Ленинградской, Липецкой, Московской, Мурманской, Новосибирской, Омской, Пензенской, Ростовской, Рязанской, Самарской, Смоленской, Свердловской, Тверской, Томской, Тульской, Тюменской областях и 150 адвокатов-защитников в Республике Бурятия, Краснодарском, Красноярском краях, г. Москва, Амурской, Воронежской, Иркутской, Курской, Ленинградской, Липецкой, Московской, Омской, Рязанской, Самарской областях.

Научная новизна диссертационного исследования проявляется в разработанной теоретической модели электронных доказательств в уголовном судопроизводстве, предусматривающей отражение ее теоретических, правовых, правоприменительных особенностей, определение перспектив в указанной сфере.

Научная новизна выражена в разработке авторской дефиниции «электронное доказательство в уголовном судопроизводстве», выявлении отличительных свойств электронных доказательств, определении генезиса формирования электронного уголовно-процессуального доказательства, установлении

специальных критериев допустимости электронного доказательства в уголовном процессе и научном обосновании их классификации, установлении направлений заимствования зарубежного опыта развития уголовно-процессуального доказывания в условиях цифровизации, представлении процессуального механизма сохранения электронных данных, имеющих отношение к уголовному делу, для обеспечения перспективы уголовно-процессуального доказывания, научно обоснованной дифференциации случаев участия специалиста при изъятии электронных носителей информации и копировании информации с них на обязательные и по усмотрению субъекта расследования, уточнении пределов ограничения конституционных прав личности при собирании электронных доказательств с учетом специфики источника электронных сведений, наличия рисков видоизменения (утраты) последних, уточнении роли суда в придании электронным сведениям юридической силы по уголовному делу и другое.

Научная новизна выражена и в положениях, выносимых на защиту.

Основные положения, выносимые на защиту.

1. Теоретико-правовую модель электронных доказательств в уголовном судопроизводстве следует рассматривать как совокупность авторских суждений, заключений, выводов о понятии, сущности электронного уголовно-процессуального доказательства, его отличительных свойствах и специальных критериях допустимости, особенностях процессуального порядка собирания электронных доказательств в целях эффективного установления обстоятельств по уголовному делу, правилах придания таким доказательствам юридической силы субъектом расследования преступления и судом в условиях цифровизации общественных отношениях.

2. Электронное доказательство – это сведения, содержащиеся в электронной среде, об обстоятельствах, имеющих значение для уголовного дела, зафиксированные средствами информационно-коммуникационных технологий в электронной форме, представленные в пригодном для восприятия человеком виде (с использованием электронных вычислительных машин и иной техники),

порядок обращения которых регулируется нормами уголовно-процессуального права.

3. Сущность электронного доказательства проявляется во взаимосвязи электронных сведений, составляющих содержание уголовно-процессуального доказательства, и формы их существования, определяемой информационно-технологической средой (устройство, система, сеть, облако). Она обуславливает наличие у электронного доказательства отличительных свойств: 1) отделимость содержания доказательственной информации от ее носителя; 2) допустимость создания множественности копий электронной информации, содержащихся на одном источнике уголовно-процессуального доказательства; 3) наличие в содержании электронного доказательства метаданных, идентифицирующих процесс происхождения и пути распространения электронных сведений; 4) функционирование технической среды формирования и существования электронного доказательства; 5) высокая подверженность электронного доказательства к изменению и (или) исчезновению.

4. К электронным доказательствам необходимо предъявлять дополнительные требования – специальные критерии допустимости, которые подлежат градации на: 1) правовые (соразмерность степени ограничения прав и свобод участников уголовного судопроизводства конституционно значимым публичным интересам, недопустимость использования в уголовно-процессуальном доказывании сведений, полученных с нарушением закона), 2) технические (аутентичность, идентифицируемость, целостность, проверяемость, воспроизводимость, защищенность), 3) регламентационные (обязательность регистрации работы с электронными доказательствами, ограничение доступа к электронным носителям электронных данных, использование сертифицированных программных средств при собирании, копировании, хранении электронных данных).

5. Обеспечению перспективы уголовно-процессуального доказывания, соблюдению законности при производстве по уголовному делу в условиях цифровизации общественных отношений будет способствовать включение в

процессуальную форму собирания следователем, дознавателем электронных доказательств:

1) механизма установления должного источника электронных сведений;

2) процессуального порядка безотлагательного сохранения электронных данных, имеющих отношение к предмету доказывания и иным, значимым для уголовного дела, обстоятельствам;

3) правил определения случаев обязательного участия специалиста в производстве следственных действий при копировании, извлечении электронных доказательств;

4) механизма фиксации характеристик электронных сведений и порядка их получения.

6. Осуществлению всесторонней и полной проверке электронных уголовно-процессуальных доказательств в ходе предварительного расследования препятствует действие ряда факторов: 1) отсутствие в частых случаях объективной возможности у следователя, дознавателя исследовать в полном объеме содержание электронного доказательства ввиду его отличительных свойств; 2) приоритетное использование властным субъектом производных форм закрепления электронной информации (скриншот, фототаблица, распечатка) взамен первоначального источника электронных сведений; 3) допущение властным участником уголовного судопроизводства вынужденных ошибок интерпретации метаданных ввиду несоответствия между собой по техническим причинам даты, времени создания и сохранения электронных сведений; 4) наличие технических препятствий для разграничения локальной памяти устройства и серверного хранения электронной информации; 5) отсутствие установленной законом формы направления запроса следователем, дознавателем в рамках расследования уголовного дела и получения ответа от операторов связи, провайдеров, владельцев социальных сетей, мессенджеров, администраторов информационных сетей, предусматривающей по выбору субъекта расследования объем детализации запрашиваемых сведений электронного характера.

Нивелировать указанные факторы возможно посредством:

а) установления правила в уголовно-процессуальном доказывании об использовании следователем, дознавателем копии электронной информации в исключительных случаях;

б) обязательного применения специальных программно-технических средств при осмотре и извлечении электронных сведений;

в) определения порядка установления источника хранения электронных сведений, нацеленного на разграничение локальной памяти устройства и серверного хранения информации посредством получения данных как с пользовательских устройств, так и с серверной инфраструктуры информационных сервисов;

г) использования единой формы запроса следователем, дознавателем в адрес операторов связи, провайдеров, владельцев интернет-сервисов, предусматривающей общие параметры и объем детализации запрашиваемых электронных сведений, определяемого субъектом расследования.

7. Предписания действующего уголовно-процессуального закона о доказывании не охватывают специальные критерии допустимости электронных доказательств, не учитывают особые требования по фиксации технических параметров электронных сведений, особенности порядка установления принадлежности цифровых аккаунтов конкретным лицам. Вследствие указанного нарушается законность при принятии итогового процессуального решения, ущемляется право личности на доступ к правосудию в разумный срок, возникают препятствия по ограждению личности от необоснованного уголовного преследования и обвинения. Для преодоления указанного необходимо на уполномоченных субъектов уголовного судопроизводства возложить процессуальную обязанность учитывать при оценивании электронного доказательства: а) целостность содержания электронных данных, составляющих содержание указанного доказательства; б) возможность изменения обозначенных данных; в) происхождение электронных сведений, имеющих значение для

уголовного дела; г) идентификацию устройства или пользователя, с которым связаны указанные сведения.

8. Особенности процессуальной формы электронных доказательств не должны влечь снижение процессуальных гарантий состязательности и равноправия сторон при представлении и исследовании указанных доказательств в судебном разбирательстве по уголовному делу, защиты личности от необоснованного обвинения и осуждения, права на доступ к правосудию. Для исключения негативных последствий использования электронных доказательств в уголовном процессе суду надлежит предпринимать действия по собиранию (при недостаточности) и проверке электронных доказательств, не ограничиваясь их формальной оценкой на основании внутреннего убеждения.

9. Формированию единообразной практики уголовно-процессуального доказывания, обеспечению законности процессуальных действий и решений в уголовном судопроизводстве, соблюдению прав личности, законных интересов организаций в условиях цифровизации общественных отношений будет способствовать совершенствование уголовно-процессуального закона путем:

– дополнения УПК РФ понятиями: «электронные данные», «электронное доказательство» (ст. 5 УПК РФ);

– включения в уголовно-процессуальный закон процессуального механизма безотлагательного сохранения электронных данных (ст. 185.1 УПК РФ);

– установления порядка предоставления по запросу следователя, дознавателя электронных данных лицом, осуществляющим их хранение или обработку (ст. 186.2 УПК РФ);

– уточнения пределов ограничения конституционных прав личности при собирании электронных доказательств с учетом специфики источника электронных сведений, наличия рисков их видоизменения, утраты (дополнение ст. 164.1 УПК РФ частями пятой, шестой; дополнение ст. 177 УПК РФ частью седьмой, ст. 186.3 УПК РФ);

– конкретизации процессуального порядка производства следственных действий, в ходе производства которых копируются, извлекаются, закрепляются электронные сведения (ст. 164.1 УПК РФ);

– уточнения условия признания электронного доказательства недопустимым – при неустановлении: а) его аутентичности, б) идентификации источника электронных данных, в) целостности (неизменности), г) воспроизводимости, д) верифицируемости, е) прослеживаемости пути обращения с электронными сведениями (дополнение ст. 75 УПК РФ частью третьей);

– конкретизации порядка проверки электронных доказательств посредством закрепления требования об обязательном установлении технического источника формирования электронных сведений (дополнение ст. 87 УПК РФ частью первой.1);

– уточнения процедуры оценки уполномоченным субъектом электронного доказательства в ходе предварительного расследования и судебного разбирательства по уголовному делу (дополнение ст. 88 УПК РФ частью первой.1) и др.

Соответствующий проект федерального закона помещен в Приложение 1 к диссертации.

Теоретическая значимость результатов исследования обусловлена тем, что положения диссертационного исследования способствуют развитию научных представлений об электронных доказательствах в уголовном судопроизводстве, уточняют содержание понятия «электронное доказательство», перечень критериев допустимости электронных доказательств, расширяют знания об оптимальном порядке собирания, закрепления, проверки и оценки электронных доказательств в ходе предварительного расследования, а также систематизируют знания об осуществлении судом проверки и оценки электронных доказательств по уголовным делам.

Результаты диссертационной работы могут быть использованы при проведении дальнейших научных исследований проблем использования электронных доказательств в уголовном судопроизводстве.

Практическая значимость результатов состоит в том, что диссертантом предложен ряд научно-практических решений, позволяющих совершенствовать нормативно-правовую базу по вопросам уголовно-процессуального доказывания в условиях цифровизации общественных отношений, в том числе посредством конкретизации критериев допустимости электронного доказательства, определения процессуального порядка безотлагательного сохранения электронных данных, имеющих значение для уголовного дела, уточнения правил проверки электронных доказательств властными субъектами уголовного процесса. В приложении к исследованию автором приведен перечень имеющих практическое значение конкретных правотворческих предложений по изменению и дополнению существующего нормативно-правового регулирования, помещены методические рекомендации по порядку закрепления электронных доказательств в уголовном судопроизводстве.

Результаты диссертационного исследования, приведенный в работе анализ теоретического и эмпирического материала могут быть использованы в учебном процессе образовательной организации по курсу «Уголовно-процессуальное право», а также в ходе профессиональной переподготовки и повышения квалификации должностных лиц органов предварительного расследования, адвокатов, осуществляющих защиту по уголовным делам.

Апробация результатов исследования. Основные положения диссертации нашли отражение в 7 научных публикациях, 3 из которых – в изданиях, рекомендованных и включенных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук, по научным специальностям, соответствующим им отраслям науки. Результаты диссертационного исследования докладывались соискателем на 10 научных мероприятиях международного, всероссийского уровней: «Человекоцентричность права: реперные точки и трансформации» (г. Казань, 2023 г.); «Российское

уголовное судопроизводство в условиях глобальных мировых процессов» (г. Москва, 2024 г.); «Особенности противодействия гибридным угрозам в отношении Российской Федерации» (г. Луганск, 2024 г.); «Принципы уголовного судопроизводства» (г. Москва, 2024 г.); «Уголовное судопроизводство: современное состояние и стратегия развития» (г. Москва, 2024 г.); «Совершенствование уголовно-процессуальных и криминалистических мер противодействия преступности» (г. Омск, 2024 г.); «Правовая система и вызовы современности» (г. Уфа, 2024 г.); «Потерпевший в уголовном процессе: проблемы уголовно-процессуальной и криминологической теории и правоприменительной практики» (г. Москва, 2025 г.); «Актуальные проблемы противодействия преступности на современном этапе» (г. Москва, 2026 г.).

Структура диссертационного исследования представлена введением, тремя главами, объединяющими 5 параграфов, заключением, библиографическим списком, приложениями.

Глава 1. Теоретико-правовые основы электронных доказательств в уголовном судопроизводстве

§ 1.1. Электронные доказательства в уголовном судопроизводстве: сущность, отличительные свойства, генезис формирования

Интенсивное развитие науки и техники в современный период формирует новые общественные отношения, затрагивающие и сферу уголовного судопроизводства. По данному поводу О. А. Малышева пишет, что «основной массив сведений, характеризующих фактические обстоятельства совершенного преступления … требуется оформлять в электронном виде»[3]. Согласно результатам эмпирического исследования следователи, дознаватели органов внутренних дел, следователи Следственного комитета России часто в доказывании по уголовным делам используют электронные доказательства. Только 3 % указанных респондентов уточнили, что не используют электронные доказательства в уголовно-процессуальном доказывании[4]. Достаточно активно сведения в электронной форме для установления имеющих значение по уголовному делу обстоятельств собирают адвокаты – защитники (92 %)[5]. Приведенные данные дополнительно подтверждают возрастающую значимость электронных доказательств в уголовно-процессуальном доказывании.

---

[3] Малышева О. А. Особенности доказывания, осуществляемого следователем, в условиях цифровизации уголовного судопроизводства // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 10 (74). С. 83.

[4] Приложение № 2 к диссертации (вопрос № 4).

[5] Приложение № 3 к диссертации (вопрос № 1).

В научной литературе по уголовному процессу сопоставляются понятия: «цифровые доказательства»[6], «электронные доказательства»[7], «цифровые (электронные) доказательства»[8]». В частности, А. Ю. Черданцев приравнивает цифровые доказательства к электронным[9]. Н. В. Олиндер отстаивает позицию о том, что понятие «электронные доказательства» является «некорректным, поскольку информация, содержащаяся в таких доказательствах представлена в цифровой форме, следовательно, речь идет о доказательствах, содержащих цифровую информацию»[10]. С. В. Калитин считает неверным смешение понятий «электронное» и «цифровое» применительно к доказательству. По его мнению, это две составляющие единого целого. Электронная часть доказательств, как полагает автор, связана только с электронными приборами или сокращенно с электроникой – техникой, использующей для работы электроны, а именно электричество. Цифровая составляющая – это информация, запрограммированная машинным кодом, построенным на двоичной или иной системе счисления[11].

Анализ вышеуказанных позиций ученых позволяет заключить, что авторы в ходе исследования понятия «электронное доказательство» преимущественно обращали внимание на одну лишь сущностную черту электронного доказательства – закрепление сведений на электронном носителе, оставляя без внимания значение других сущностных черт, которые характерны для данного

---

[6] Карташов И. И. Проблемы формирования доказательств в уголовном судопроизводстве на основе электронной информации // Юридическая наука. 2018. № 3. С. 99-103; Облаков А.А. Цифровые доказательства в уголовном процессе: проблемы сбора и оценки // Закон и власть. 2024. № 5. С. 158. Рамалданов Х. Х. Проблемы использования и хранения цифровых доказательств в доказывании в уголовном процессе // Вестник Казанского юридического института МВД России. 2023. Т. 14. № 2 (52). С. 107; Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12. № 5. С. 202.

[7] Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / под ред. С. В. Зуев. М., 2024. С. 11.

[8] Черецких А. В. Электронные (электронные) доказательства в уголовном судопроизводстве // Правопорядок: история, теория, практика. 2023. № 4 (39). С. 110-117.

[9] Черданцев А. Ю. Понятие электронных доказательств, современное состояние и их роль в доказательственном процессе // Юридическая наука и практика. 2019. № 4. С. 59.

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

[11] Калитин С. В. Доказательства электронные и электронные // Научно-методический электронный журнал Концепт. 2014. Т. 20. С. 3587-3588.

вида доказательства. Сущность электронных доказательств в уголовном процессе действительно характеризуется определенной двойственностью. С одной стороны, электронные доказательства ассоциируются с физическими устройствами: компьютеры, компакт-диски и флэш-накопители, которые содержат электронную информацию и могут быть представлены в суд. Такое понимание электронного доказательства отражено в правовой позиции Верховного Суда Российской Федерации, выраженной в Постановлении Пленума Верховного Суда Российской Федерации от 26.12.2017 № 57. В частности, Верховный Суд Российской Федерации указывает на допустимость подачи в электронном виде документов в суд[12].

Как отмечают Г. С. Русман и С. В. Сурменева, в уголовном судопроизводстве все более распространенными становятся электронные документы. Это могут быть доказательства в уголовном деле, иные документы (характеристики, справки, ответы на запросы, полученные следователем в электронном виде, напечатанный с использованием компьютера протокол следственного действия и другие)[13]. Одновременно, в судебной практике отмечаются нередкие факты отнесения к электронным доказательствам не только данных, хранящихся на физических носителях, но и различные формы электронной информации: электронные сообщения, документы в электронной форме, электронные аудио- и видеозаписи, фотоизображения, информация с интернет-порталов публичных органов и организаций, контент из СМИ, SMS-сообщения, данные из бизнес-мессенджеров и социальных сетей, а также электронные копии документов и электронные отпечатки сайтов (веб-архивы)[14].

---

[12] Постановления Пленума Верховного Суда Российской Федерации от 26 декабря 2017 года № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // СПС «КонсультантПлюс» (дата обращения: 05.01.2026).

[13] Русман Г. С., Сурменева С. В. Цифровые инструменты в примирительных процедурах уголовного судопроизводства: современное состояние и перспективы // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: материалы международной научно-практической конференции. СПб., 2023. С. 257.

[14] Апелляционные определения Верховного Суда Российской Федерации от 01 августа 2019 года № 67-АПУ19-8; от 13 декабря 2018 года № 4-АПУ18-41 // ГАС «Правосудие» (дата обращения: 10.01.2026).

Отмеченное свидетельствует о необходимости адаптации уголовно-процессуального законодательства и правоприменительной практики к быстро меняющимся в технологическом плане общественным отношениям и формам хранения данных.

В УПК РФ содержится закрытый перечень видов доказательств, что, по мнению Л. В. Головко, имеет как преимущества, так и недостатки. Основное достоинство такого перечня, как считает ученый, заключается в том, что предотвращается включение в материалы уголовного дела ненадежной и низкокачественной информации. Существенным недостатком отмеченной правовой регламентаций перечня видов уголовно-процессуальных доказательств является неспособность этого списка соответствовать быстрому развитию технологий и появлению новых видов информации – данных из социальных сетей и интернета[15].

Позиция Л. В. Головко обоснованно подчеркивает ценность закрытого перечня уголовно-процессуальных доказательств как процессуальной гарантии качества и надежности доказательственной информации в уголовном судопроизводстве. Вместе с тем указанная гарантия не согласуется с объективной потребностью в адаптации доказательственного права в уголовном процессе к электронной виртуальной среде: электронные сведения не должны исключаться из процесса доказывания. Требуется уточнение их сущности, процессуальной формы использования в уголовном судопроизводстве. Задача состоит не в формальном расширении перечня видов уголовно-процессуальных доказательств, а в разработке понятия и конкретизации свойств электронных доказательств, определения процессуальных правил их получения, закрепления следователем, дознавателем, надлежащей проверки и оценки субъектом расследования, судом в целях формирования с учетом современного развития общественных отношений перечня доказательств, предусмотренного ч. 2 ст. 74 УПК РФ, предполагающего

[15] Головко Л. В. Курс уголовного процесса / под ред. Л. В. Головко. М. .: Статут, 2016. С.444.

включение электронных сведений в систему уголовно-процессуальных доказательств.

Многие ученые-процессуалисты рассматривают понятие «доказательство» как единство фактических сведений и процессуальной формы их получения. П. А. Лупинская отмечала, что «доказательство по уголовному делу выступает в единстве своего содержания (фактических данных) и процессуальной формы (источник получения фактических данных)»[16]. С. А. Шейфер уточнял, что «показания, заключения, вещественные доказательства, протоколы и документы являются доказательствами, но рассматриваемыми со стороны их формы, в то время как сведения о фактах, подлежащих доказыванию, составляют содержание доказательств. Синтезированное же определение уголовно-процессуальное доказательство будет звучать так: доказательство – это сведения об обстоятельствах, подлежащих доказыванию, полученные законным способом и облеченные в надлежащую процессуальную форму – в форму показаний, заключений и др.»[17]. Схожее понятие доказательства предлагает Р. В. Костенко[18]. Критикуя положения ст. 74 УПК РФ, А. Р. Белкин указывает, что «само доказательство (как содержание) и источник доказательства (как форма) совершенно разные понятия. Доказательство, по его мнению, имеет содержательную и формальную стороны»[19].

В развитие указанного следует уточнить, что в ходе доказывания следователь, дознаватель, суд осуществляют легализацию имеющих значения для уголовного дела сведений посредством отнесения их к предусмотренному уголовно-процессуальным законом виду доказательства. В данной связи заслуживает внимания мнение Л. А. Воскобитовой о том, что «современное представление о доказательстве в уголовном процессе формировалось постепенно

---

[16] Уголовно-процессуальное право Российской Федерации: учебник / отв. ред. П. А. Лупинская, Л. А. Воскобитова. М.: Норма: ИНФРА-М, 2024. С. 289.

[17] Шейфер С. А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования : монография. М.: Норма, 2009. С. 7.

[18] Костенко Р. В. Доказательства в уголовном процессе: концептуальные подходы и перспективы правового регулирования : дис. … д-ра юрид. наук. Краснодар, 2006. С. 109.

[19] Белкин А. Р. Еще раз о доказательствах, об источниках доказательств и о том, как отличить одно от другого // Мировой судья. 2012. № 1. С. 10-15.

от интуитивного понимания, … до современных размышлений о трансформации доказывания при использовании электронных технологий и современной дискуссии по вопросу, а не появился ли новый вид доказательств – “электронные доказательства”»[20].

В ч. 1 ст. 74 УПК РФ законодателем определяется понятие доказательства, в части 2 указанной статьи уголовно-процессуального закона – источники доказательств. Обозначенные перечень источников не включает электронные сведения, позволяющие установить наличие или отсутствие обстоятельств, имеющих значение для уголовного дела. Согласно положениям теории уголовно-процессуального права доказательствами по уголовному делу могут быть признаны не любые сведения[21], что указано в ч. 1 ст. 74 УПК РФ, а только те, которые получены из источников, предусмотренных ч. 2 ст. 74 УПК РФ, и которые не противоречат требованиям, закрепленным уголовно-процессуальными нормами (ст.ст. 76-81, 83, 84 и 88 УПК РФ). Уголовно-процессуальное законодательство не закрепляет понятие «электронное доказательство», что порождает неопределенность в правоприменительной практике и возможность разнообразного толкования предписаний уголовно-процессуального закона, что недопустимо в силу ч. 1 ст. 2 УПК РФ. В отдельных нормах УПК РФ встречаются понятия: «электронные носители информации» (ст. 164.1 УПК РФ), «электронные сообщения» (ст. 185 УПК РФ). Однако в ст. 74 УПК РФ они не указываются.

Несмотря на отсутствие легального определения термина «электронное доказательство», данное понятие часто становится объектом исследования многих процессуалистов. Понятие «электронное доказательство» – исключительно доктринальное. УПК РФ регламентирует особенности изъятия электронных носителей информации и копирования с них электронной информации при

---

[20] Воскобитова Л. А. Понятие доказательства и использование «электронной» информации в доказывании по уголовному делу // Высокотехнологичное право: современные вызовы: Материалы IV Международной межвузовской научно-практической конференции. Красноярск, 2023. С. 57-58.

[21] Рамалданов Х. Х. Процесс доказывания по уголовным делам в условиях тотальной цифровизации общественных отношений : дис. … канд. юрид. наук. М., 2024. С. 25.

производстве следственных действий. В отечественной юридической литературе сформировались несколько направлений осмысления данного понятия: процессуально-информационное, технико-цифровое, материалистическое и нормативно-понятийное.

По мнению М. И. Воронина, «электронными доказательствами являются сведения, содержащиеся в электронном документе и/или на электронном носителе информации, на основании которых субъекты доказывания устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела»[22]. Данное определение заслуживает внимания, поскольку отражает стремление автора адаптировать классическую теорию доказательств к процессу цифровизации. Следует поддержать М. И. Воронина в том, что им делается акцент на содержание, а не форму доказательства. Ученый подчеркивает, что электронные доказательства – это прежде всего сведения, а не просто материальные объекты. Таким образом, М. И. Воронин последовательно отстаивает: 1) информационный характер доказательства; 2) комплексность источников электронных доказательств. Отмеченное распространяется не только на документы с электронной подписью, но и на видеозаписи, аудиофайлы, записи видеорегистраторов, переписку в сети и другие формы хранения данных.

Вместе с тем сложно полностью согласиться с предложенным М. И. Ворониным понятием электронного доказательства, поскольку в нем: 1) отсутствует указание на сущностные черты электронного доказательства – на их электронную (нематериальную) природу, возможность их копирования и изменяемости, необходимость сохранения целостности. Без такого уточнения электронное доказательство становится тождественным доказательству, например иному документу, и теряет свою особенность; 2) отмечается размытость границ между электронным документом и электронным носителем информации. В дефиниции М.И. Воронина указано «и/или на электронном носителе

[22] Воронин М. И. Электронные доказательства в УПК: быть или не быть? // Lex russica. 2019. № 7 (152). С. 79.

информации». Однако электронный документ всегда хранится на каком-либо носителе (жесткий диск, флеш-память, облако и т.д.). Следовательно, эти категории частично пересекаются, а их одновременное упоминание избыточно и может вызвать сложности при производстве по уголовному делу; 3) отсутствует акцент на свойства электронного доказательства: достоверность и аутентичность, а именно на необходимость подтверждения подлинности электронных данных или их идентификации (например, через электронную подпись, хэш-сумму, метаданные). Кроме того, именно свойство проверяемость отличает электронное доказательство от обычной электронной информации; 4) не обозначается требование процессуального закрепления. Между тем допустимость электронных доказательств зависит прежде всего от того, как они закреплены в ходе производства по уголовному делу; 5) требуется конкретизировать для лучшего восприятия правоприменителем отличия электронного доказательства от других источников уголовно-процессуальных доказательств.

Таким образом, формирование М. И. Ворониным понятия электронного доказательства представляет собой важный этап в теоретическом осмыслении феномена электронных доказательств. Его достоинство – сохранение преемственности с классической концепцией доказательств и попытка институционализировать электронную форму информации в уголовном процессе. Однако для нормативного и практического использования анализируемой категории требуют уточнения дефиниция электронного доказательства, его свойств, процессуального порядка закрепления.

Научный интерес в данной связи представляет позиция В. Б. Вехова, который определяет электронные доказательства как «любые сведения (сообщения, данные), представленные в электронной форме, на основе которых суд, прокурор, дознаватель в определенном процессуальном законодательством порядке устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств,

имеющих значение для правильного рассмотрения и разрешения дела»[23]. В. Б. Вехов основывается на доктрине доказательств: электронная форма лишь видоизменяет способ существования доказательства**,** не создавая новую правовую категорию. Достоинство представленной научной позиции – процессуальная четкость. Вместе с тем следует отметить отсутствие в ней акцента на особые черты электронной среды (метаданные, сетевое хранение, изменяемость, зависимость от технических средств).

О. В. Журкина предлагает иной взгляд на определение электронного доказательства, характеризуя его как «сведения, выраженные в электронно-цифровом виде, содержащиеся на электронных носителях, для представления которых необходимо программное обеспечение, хранящиеся в компьютерной сети и (или) передаваемые через нее»[24]. Ученый концентрируется на технической сущности электронных данных. Автор надлежаще указывает на важнейшие характеристики электронного доказательства: электронный формат, зависимость от программного обеспечения и сетевое существование информации. Положительной стороной данного определения является его современность и технологическая конкретизация. Однако дефиниция О. В. Журкиной отличается избыточностью технических характеристик при недостаточности процессуальной составляющей: в ней отсутствует указание на участие субъектов доказывания, правила получения данных, их закрепления. Определение детализирует форму, но не раскрывает юридическое содержание доказательства.

М. В. Горелов рассматривает электронные доказательства в качестве «сведений об обстоятельствах, имеющих значение для дела, выполненные в форме электронной, звуковой и видеозаписи». К электронным доказательствам, указанный автор также относит выполненные с помощью электронно-вычислительных средств протоколы судебных заседаний, протоколы совершения

---

[23] Вехов В. Б. Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2001. № 4 (11). С. 47.

[24] Журкина О. В. Электронные доказательства: понятие и признаки // Российская юстиция. 2020. № 9. С. 45.

отдельных процессуальных действий[25]. Эта позиция интересна тем, что автор рассматривает электронные доказательства через особые способы закрепления информации. Положительным аспектом представляемой позиции является практическая наглядность: определение охватывает конкретные формы, уже используемые в правоприменении (видео- и аудиозаписи, электронные протоколы). Тем не менее, теоретически данная позиция недостаточно обоснована. Электронная, звуковая и видеозаписи – это технические способы закрепления информации, а не самостоятельные категории теории уголовно-процессуального доказывания. Как представляется, М. В. Горелов подменяет сущность электронного доказательства признаками формы, не раскрывая самостоятельной сущности анализируемого доказательства. Электронный формат является лишь характеристикой носителя, а не критерием нового вида доказательственной информации.

Иную позицию высказывает Р. И. Оконенко, полагающий, что «под электронным доказательством понимается электронный носитель информации, содержащий сведения о значимых обстоятельствах по конкретному уголовному делу и обладающий следующими юридически значимыми признаками: а) значительным объемом памяти; б) простотой передачи и копирования сведений с одного электронного носителя информации на другой; в) возможностью удаленного доступа к содержанию электронного носителя и информационно-телекоммуникационным системам (в частности, к сети «Интернет»); г) относительностью и неочевидностью содержания»[26]. Отождествление носителя информации и содержания сведений указанным ученым противоречит сущности доказательства – сведения о фактах. Более того, упомянутые признаки электронного доказательства характеризуют правила хранения и передачи сведений. Таким образом, позиция

[25] Горелов М. В. Электронные доказательства в гражданском судопроизводстве России: вопросы теории и практики : автореф. дис. … канд. юрид. наук. Екатеринбург, 2005. С. 8.

[26] Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. … канд. юрид. наук. М, 2016. С. 64.

Р. И. Оконенко больше применима в криминалистике, чем к системе уголовно-процессуальных понятий.

Обобщение предлагаемых дефиниций электронного доказательства свидетельствует об отсутствии в отечественной науке уголовного процесса единого понятия электронного доказательства. Общей тенденцией является стремление ученых объединить два принципиальных начала: 1**)** информационно-правовое (сведения как доказательство по смыслу ч. 1 ст. 74 УПК РФ); 2) технико-электронное (особая форма существования и механизм закрепления электронных данных).

В развитие указанного подчеркнем, что электронные доказательства учеными предлагается рассматривать как вещественные доказательства[27] и иные документы[28] в зависимости от оформления информации, ее хранения, использования в совершении преступлений[29], отдельный вид доказательства, что обусловлено их сущностью, которая заключается, в первую очередь, в носителе электронных данных[30] – отдельном, искусственно обособленном источнике сведений о фактах, которые могут использоваться в качестве доказательств в

---

[27] Пастухов П. С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: автореф. дис. … д-ра юрид. наук. М., 2015. С. 13.

[28] Рыбин А. В. Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации: процессуальные и криминалистические аспекты: дис. ... канд. юрид. наук. Краснодар, 2005. С. 11-13.

[29] Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. № 3 (26). С. 49; Калиновский К. Б., Маркелова Т. Ю. Доказательственное значение «электронной» информации в российском уголовном процессе // Российский следователь. 2001. № 6. С. 18-19; Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании: учебное пособие / под ред. Ю. В. Гаврилина и А. В. Победкина. М. : Академия управления МВД России, 2021. С. 41; Маламагамедова А. Р. «Электронные доказательства» в уголовном процессе // Уголовная политика России на современном этапе: состояние, тенденции, перспективы: Сборник научных трудов по материалам международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Г. А. Аванесова. В 2-х частях. М., 2024. С. 291.

[30] Бикмиев Р. Г., Бурганов Р. С. Собирание электронных доказательств в уголовном судопроизводстве // Информационное Право. 2015. № 3. С. 18; Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: дис. … канд. юрид. наук. Челябинск, 2010. С. 210.

уголовном судопроизводстве[31], информационным доказательством[32]. Высказывается противоположная точка зрения – об отсутствии необходимости признания нового вида доказательств[33]. Однако считаем обоснованной позицию Г. С. Русман и С. В. Сурменевой о необходимости изменения существующей парадигмы уголовного процесса, связанного с внедрением технологий электронного судопроизводства и его элементов: различные цифровые и электронные порталы, сервисы, цифровые платформы и др.[34].

Анализ уголовно-процессуальной практики[35] свидетельствует, что следователи, дознаватели по-разному оценивают значение электронных сведений для установления фактических обстоятельств. В одном случае в ходе расследования уголовного дела о незаконном обороте наркотических средств следователь, осмотрев письма из электронного почтового ящика, распечатал их и приобщил к материалам уголовного дела в качестве иных документов. В другом случае электронные сведения, обнаруженные после возбуждения уголовного дела по факту получения взятки, были признаны следователем вещественным доказательством по уголовному делу. Результаты эмпирического исследования демонстрируют также, что 56 % опрошенных следователей, дознавателей электронное доказательство рассматривают в качестве вещественного

---

[31] Шаталов А. С. Роль, сущность и значение электронных (электронных) доказательств в уголовном судопроизводстве // Вестник Томского государственного университета. 2024. № 500. С. 233.

[32] Рогава И. Г., Датумян С. С., Куренная А. А. Цифровые доказательства в российском уголовном процессе: история, проблемы и перспективы развития // Проблемы экономики и юридической практики. 2021. Т. 17. № 1. С. 245.

[33] Головко Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. С. 22; Колдин В. Я. Электронная информация в праве // Вестник Московского университета. Серия 11: Право. 2016. № 2. С. 109; Химичева О. В. Следственные действия: о цифровой транс формации их производства // Криминологический журнал. 2023. № 2. С. 172.

[34] Русман Г. С., Сурменева С. В. Цифровые инструменты в примирительных процедурах уголовного судопроизводства: современное состояние и перспективы // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: материалы международной научно-практической конференции. СПб., 2023. С. 259.

[35] См. Материалы уголовного дела № 12302520006000129. СУ СК России по Омской области; материалы уголовного дела № 12302520006000081. СУ СК России по Омской области; материалы уголовного дела № 12501009625000116. ЛУ МВД России в аэропорту Шереметьево; материалы уголовного дела 12501280014000105 МСО СУ СК РФ по Тверской области.

доказательства. Порядка четверти респондентов отметили необходимость самостоятельного закрепления рассматриваемого доказательства в ч. 1 ст. 74 УПК РФ[36]. Аналогичное мнение высказали 48 % опрошенных адвокатов-защитников[37]. Отмеченное свидетельствует об отсутствии единообразной практики отнесения электронных доказательств к определенному виду доказательств согласно ч. 2 ст. 74 УПК РФ. Это нарушает принцип правовой определенности, признаваемый Конституционным Судом Российской Федерации в качестве элемента права на справедливое судебное разбирательство[38].

Раскрывая сущность электронного доказательства, следует уточнить, что электронная доказательственная информация обладает отличительными признаками, которые не свойственны ни вещественным доказательствам, ни иным документам, посредством которых устанавливаются фактические обстоятельства совершенного преступления. При отнесении электронных сведений к вещественным доказательствам акцент при оценке первого делается на материальный носитель (устройство, накопитель), тогда как доказательственное значение чаще имеет не сам предмет (материальный носитель), а сведения, которые могут быть отделены от носителя, многократно воспроизведены и перенесены без видимых изменений.

При отнесении электронных сведений к иным документам доминирующей при оценке такого доказательства становится документарная форма последнего (структура документа, реквизиты, создатель документа), тогда как отличительным признаком электронных сведений является наличие их связи с виртуальной средой формирования и хранения таких сведений, метаданными, что выходит за пределы традиционного понимания уголовно-процессуального доказательства в виде иного документа. Значительная часть электронных сведений не отвечает требованиям,

---

[36] Приложение № 2 к диссертации (вопрос № 4).

[37] Приложение № 3 к диссертации (вопрос № 2).

[38] Постановление Конституционного Суда Российской Федерации от 09 июля 2020 года № 34-П «По делу о проверке конституционности части второй статьи 313 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой администрации муниципального образования город Мурманск» // СПС «КонсультантПлюс» (дата обращения: 28.04.2026).

присущим документу в классическом понимании. Например, лог-файлы формируются автоматически, поэтому не имеют упорядоченную структуру, сведения о соединениях абонентов генерируются техническими системами и как метаданные не имеют самостоятельного автора, но имеют важное доказательственное значение.

Дополнительным аргументом о необходимости включения в ст. 74 УПК РФ электронного доказательства является наличие у него особого предмета проверки, который отсутствует применительно к доказательствам. Если для последних достаточным является установление относимости, допустимости и достоверности, то в отношении электронных доказательств дополнительно подлежат установлению: аутентичность (подлинность источника, содержащего электронного сведения), целостность (отсутствие изменений электронных сведений), идентифицируемость (возможность определения связи с конкретным субъектом или устройством, соответственно владеющим, содержащим электронные сведения), воспроизводимость с сохранением неизменности содержания. Важность учета обозначенных признаков электронных доказательств отмечается как в научной литературе[39], так и в правовых позициях Верховного Суда Российской Федерации. Так, высший суд в своих разъяснениях неоднократно указывал на необходимость оценки электронных доказательств с учетом возможности их изменения и необходимости установления источника происхождения (в частности, при оценке переписки, данных биллинга, информации из сети Интернет)[40].

---

[39] Квасница С. Е., Бирюков С. Ю. Электронные доказательства: проблемы допусти мости в уголовном судопроизводстве // Вестник Волгоградской академии МВД России. 2024. № 2 (69). С. 101; Никурадзе Н. О. К вопросу об оценке «электронных доказательств» в уголовном судопроизводстве в контексте российского и зарубежного опыта // Вестник Томского государственного университета. 2024. № 508. С. 267; Зуев С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 621.

[40] Постановление Пленума Верховного Суда Российской Федерации от 26 декабря 2017 года № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов»; от 23 апреля 2019 года № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» (дата обращения: 05.05.2026).

Таким образом, сущность электронных доказательств заключается не только в форме представления электронных сведений, но и в наличии дополнительных, технологически обусловленных способов получения, критериев их проверки и оценки. В силу указанных обстоятельств электронное доказательство целесообразно рассматривать как самостоятельный вид уголовно-процессуального доказательства.

В теории уголовно-процессуального права общепризнанным является положение о том, что любое доказательство должно отвечать ряду универсальных требований. В развитие указанного В. А. Лазарева[41], П. А. Лупинская[42], А. В. Смирнов[43], С. А. Шейфер[44] уточняли, что свойствами уголовно-процессуальных доказательств выступают относимость, допустимость и достоверность. Обозначенные свойства являются универсальными и присущи, в том числе, электронным доказательствам.

Подчеркнем, что относимость уголовно-процессуального доказательства – это способность сведений подтверждать или опровергать обстоятельства, предусмотренные ст. 73 УПК РФ, а также иные обстоятельства, имеющие значение для уголовного дела. Допустимость – это свойство доказательства, характеризующее его с точки зрения законности источника фактических данных (сведений, информации), а также способов получения и форм закрепления фактических данных, содержащихся в таком источнике, в порядке, предусмотренном уголовно-процессуальным законом, т. е. управомоченным на то лицом или органом в результате проведения им следственного действия при строгом соблюдении уголовно-процессуального закона, определяющего процессуальную форму данного следственного действия[45]. Свойство

---

[41] Лазарева В. А. Доказывание в уголовном процессе. М.: Юрайт, 2009. С. 145.

[42] Уголовно-процессуальное право РФ : учебник / отв. ред. П. А. Лупинская. М.: Норма, 2011. С. 298.

[43] Смирнов А. В., Калиновский К.Б. Уголовный процесс: учебник для вузов. М.: Норма: ИНФРА-М, 2022. С. 220.

[44] Шейфер С. А. Сущность и способы собирания доказательств в советском уголовном процессе. М.: Изд-во Саратовского университета, 1972. С. 34.

[45] Кипнис Н. М. Допустимость доказательств в уголовном судопроизводстве / отв. ред. П. А. Лупинская. М.: Юрист, 1995. С. 27.

«достоверность» означает соответствие электронных сведений фактической действительности.

Особенности электронной (виртуальной) среды существования электронных данных обусловливает наличие у электронных доказательств особых, отличительных свойств. К их числу следует отнести:

1) нематериальный характер доказательственной информации при наличии материального носителя. В отличие от вещественных доказательств, где содержание неотделимо от предмета, электронные данные могут существовать независимо от конкретного носителя;

2) допустимость создания множественности идентичных копий электронной информации. Электронная информация может быть скопирована без изменения ее содержания, при этом копия при соблюдении определенных технических условий является по сути тождественной оригиналу электронной информации. Данное свойство отделяет электронное доказательство от иных документов и вещественных доказательств;

3) наличие в содержании электронного доказательства метаданных. В электронной среде значимыми являются не только сами сведения (текст, изображение), но и связанные с ними данные (время создания текста, изображения, его изменения, сведения об устройстве с которого получена электронная информация). Наличие метаданных позволяет проанализировать происхождение и пути распространения электронных сведений;

4) техническая среда формирования и существования электронного доказательства. Электронные доказательства возникают, хранятся и воспроизводятся исключительно с использованием технических средств и программного обеспечения. Это обусловливает необходимость в более частых случаях привлечения специалистов и экспертов, что не является обязательным при получении большинства традиционных доказательств;

5) большая подверженность изменению, исчезновению.

Выделение отличительных свойств электронных доказательств имеет теоретическое и практическое значение. Оно подтверждает, что без нормативного

закрепления всех свойств (общих, отличительных) электронных доказательств невозможно обеспечить единообразную их оценку, исключить ошибки в уголовно-процессуальной деятельности при использовании электронных доказательств следователем, дознавателем, судом при установлении фактических обстоятельств.

Приведенная градация свойств электронных доказательств, а также выявление их сущности позволяет предложить авторское определение электронного доказательства. Под ним следует понимать сведения, содержащиеся в электронной среде, об обстоятельствах, имеющих значение для уголовного дела, зафиксированные средствами информационно-коммуникационных технологий в пригодном для восприятия человеком виде (с использованием электронных вычислительных машин и иной техники), порядок обращения которых регулируется нормами уголовно-процессуального права. Данное определение включает процессуальный, информационный, технический и процессуальный аспекты дефиниции электронного доказательства, существование которого обусловлено интенсивной цифровизацией общественных отношений.

Анализируя особенности использования электронных доказательств в уголовном судопроизводстве, следует акцентировать внимание на процесс формирования указанного доказательства. В данном случае, основываясь на положениях теории доказательств о том, что сведения об обстоятельствах, имеющих значение для уголовного дела, приобретают статус доказательства только при условии их получения и закрепления в предусмотренной законом процессуальной форме[46], следует выделить два самостоятельных, но взаимосвязанных способа формирования электронного доказательства:
1) возникновение электронной информации вне уголовного процесса;
2) придание электронной информации доказательственного значения властным субъектом уголовного судопроизводства.

В первом случае электронные сведения возникают в результате деятельности пользователей электронных ресурсов (переписка, файлы) либо

[46] Телевицкая Ю. А. Выемка электронных носителей информации по уголовным делам : дис. … канд. юрид. наук. Н. Новгород, 2023. С. 66.

автоматически (логи[47], биллинг[48]). В рассматриваемый период времени такие сведения не являются доказательствами, а могут таковыми стать при облечении их в процессуальную форму, если отвечают свойству относимости.

Во втором случае осуществляется внедрение электронных сведений в уголовное судопроизводство уполномоченным субъектом посредством осуществления предусмотренных уголовно-процессуальным законом процессуальных действий. Таким образом формируется уголовно-процессуальное доказательство. При этом возможны различные способы придания электронным сведениям статуса доказательства, что и порождает отмеченную выше неопределенность.

Если электронные данные включаются в уголовный процесс после их оформления в виде документа, полученного от организации, распечатки переписки между участниками уголовного судопроизводства, выписки о сведениях от операторов мобильной связи, то они могут приобретать статус доказательства – иного документа при условии соблюдения требований ст. 84 УПК РФ. Однако и в этом случае доказательственное значение электронных сведений не возникает автоматически, поскольку следователь обязан процессуальным путем проверить источник их происхождения, условия формирования, неизменность таких сведений. В случае, если электронные данные появляются в уголовном судопроизводстве непосредственно в ходе процессуальной деятельности (в ходе осмотра, обыска, выемки, копирования информации), то доказательственное значение они приобретают при составлении протокола соответствующего следственного действия (ст. 164, 176, 177 УПК РФ), в котором фиксируются обстоятельства обнаружения рассматриваемых сведений, порядок их извлечения, технические характеристики носителя электронных

[47] Лог – файл с записями о событиях в хронологическом порядке. [Электронный ресурс]. URL: https://dic.academic.ru/dic.nsf/ruwiki/1008755?ysclid=morqk2995a74679376 (дата обращения: 05.05.2026).

[48] Биллинг – специальная совокупность процедур и решений, связанных со сбором информации об использовании телекоммуникационных услуг, с их тарификацией, а также с выставлением счетов абонентам и обработкой платежей. [Электронный ресурс]. URL: https://ru.wiktionary.org/wiki/%D0%B1%D0%B8%D0%BB%D0%BB%D0%B8%D0%BD%D0%B3?ysclid=morqh14hjn113520015 (дата обращения: 05.05.2026).

данных, сведения, обеспечивающие проверяемость данных (например контрольные хэш-суммы для скопированных файлов, серийный номер и модель носителя, время и дата извлечения и т.д.). Таким образом, в одном случае электронные данные внедряются в процесс в форме иного документа, предусмотренного ч. 2 ст. 74 УПК РФ, в другом случае – формируются как доказательство посредством составления протокола следственного действия. Однако указанное различие не означает существования двух разных по своей сущности доказательств. В обоих случаях речь идет об одних и тех же электронных данных, которые приобретают доказательственное значение, но имеют разное процессуальное закрепление.

Учитывая изложенное, следует подчеркнуть, что некорректным является суждение о формировании электронного доказательства исключительно вне или в ходе уголовного судопроизводства. Вне уголовного процесса формируются лишь электронные сведения, создающие фундамент потенциального доказательства. Электронное доказательство же возникает исключительно в рамках уголовно-процессуальной деятельности при производстве уполномоченным субъектом процессуальных действий.

В отличие от доказательств, источник которых является единообразным (например, показания обвиняемого оформляются протоколом допроса), электронные данные могут иметь различные источники происхождения. Они представляют собой систему взаимосвязанных процессуальных и технических средств, обеспечивающих собирание, закрепление, сохранность, проверяемость электронных данных. Указанное обстоятельство дополнительно конкретизирует сущность, отличия электронных доказательств от доказательств, предусмотренных УПК РФ.

Как отмечено ранее, согласно теории уголовно-процессуальных доказательств необходимо строго разграничивать содержание доказательства (сведения) и его форму (источник). В условиях цифровой среды данное разграничение приобретает важное значение для правоприменителя, обусловленное потребностью уточнения понятия электронных данных. Под

такими данными следует понимать сведения, существующие в электронной форме и создаваемые, хранимые, передаваемые с использованием информационных систем и сетей. Предлагаемая дефиниция охватывает широкий перечень информации без связи с ее доказательственным значением. Он основывается на содержании Конвенции о киберпреступности 2001 г.[49], включающей понятие «computer data», что следует расценивать электронные данные – категория, содержащая информацию, могущую впоследствии стать доказательством по уголовному делу. Данный подход соответствует позиции, сформулированной в работах Е. Р. Россинской[50], В. А. Мещерякова[51], рассматривающих цифровую информацию как особый вид криминалистически значимых сведений.

На основании изложенного можно сформулировать следующие выводы.

1. Электронные доказательства являются самостоятельным средством доказывания, обладающим особой сущностью в сравнении с иными видами доказательства. Отсутствие легального определения электронного доказательства в уголовно-процессуальном законе обуславливает отсутствие правовой регламентации порядка их собирания, закрепления, проверки, оценки, приводящего к формированию разнородной практики их использования в уголовно-процессуальном доказывании. Для нивелирования указанного требуется законодательное закрепление понятия «электронное доказательство» в УПК РФ.

2. Электронные доказательства характеризуются особыми свойствами, учет которых необходим для обеспечения всесторонности, полноты, объективности установления фактических обстоятельств по уголовному делу.

3. Включение электронных доказательств в ст. 74 УПК РФ обеспечит правовую определенность их содержания и значения, предотвратит ошибки

---

[49] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23.11.2001) // СПС «КонсультантПлюс» (дата обращения: 05.01.2026).

[50] Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 5 (57). С. 35.

[51] Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: ВГУ, 2002. С. 104.

уголовно-процессуальной практики в связи с уголовно-процессуальным доказыванием, усилит гарантии прав участников уголовного судопроизводства в условиях цифровой трансформации.

§ 1.2. Критерии допустимости электронного доказательства в уголовном судопроизводстве

Допустимость доказательства выступает важной гарантией объективного установления обстоятельств уголовного дела. В соответствии со ст. 75 УПК РФ каждое доказательство подлежит проверке на соответствие требованиям допустимости, что обеспечивает соблюдение принципа законности при производстве по уголовным делам. Согласно предписаниям ч. 2 ст. 50 Конституции Российской Федерации при осуществлении правосудия не допускается использование доказательств, которые были получены с нарушением норм действующего законодательства[52].

УПК РФ не содержит понятия «допустимость доказательства», легализуя лишь категорию «недопустимые доказательства». В связи с этим в уголовно-процессуальной практике правоприменители ориентируются на разъяснения Пленума Верховного Суда Российской Федерации, согласно которым доказательства признаются допустимыми, если не нарушаются конституционные права и свободы, установленный законом порядок их получения, доказательства

[52] Конституция Российской Федерации от 12 декабря 1993 года // СПС «КонсультантПлюс» (дата обращения: 03.11.2025).

получены надлежащим субъектом[53]. Аналогичная позиция отмечается и в решениях Конституционного Суда Российской Федерации.

На актуальность вопроса об определении допустимости электронных доказательств обращает внимание О.А. Малышева, отмечая, что несмотря на исследования ученых (А. А. Балашова, Р. С. Бурганов, В. Б. Вехов, О. В. Волынская, П. С. Пастухов и др.) в области получения, закрепления и оценки электронных доказательств в уголовном процессе, сложности практического характера в досудебном производстве сохраняются. Они связаны с отсутствием четких критериев допустимости электронных доказательств[54]. По результатам проведенного диссертантом эмпирического исследования было установлено, что 66 % следователей и дознавателей также указали на отсутствие четких критериев допустимости электронных доказательств и необходимость их дополнительного определения[55]. Как справедливо указывают Г. С. Русман и М. С. Смолин, цифровизация уголовного процесса влечет новые ограничения для профессиональных участников судопроизводства[56].

Следовательно, необходима выработка и нормативное закрепление единых критериев допустимости электронных доказательств, что позволит обеспечить неизменность, воспроизводимость последних, единообразие процедуры признания властным субъектом уголовного судопроизводства электронного доказательства допустимым, минимизировав тем самым риски субъективного

---

[53] Постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 года «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» // СПС «КонсультантПлюс» (дата обращения: 03.11.2025).

[54] Малышева О. А. Трансформация досудебного уголовного производства в условиях цифровизации: тенденции и риски // Тенденции уголовной политики России на современном этапе развития общества: Сборник статей Всероссийской научно-практической конференции, посвященной 25-летию кафедр уголовного права и криминологии, уголовного процесса и правоохранительной деятельности. Ижевск, 2024. С. 46-47.

[55] Приложение № 2 к диссертации (вопрос № 14).

[56] Русман Г. С., Смолин М. С. Правомочия стороны защиты в цифровом уголовном судопроизводстве // Правопорядок: история, теория, практика. 2026. № 1 (48). С. 168.

усмотрения в ходе такого признания. Схожую позицию ранее выражали А. А. Балашова[57], О. В. Желева[58], С. В. Зуев[59], В. П. Гмурко[60], А. Ю. Отченаш[61].

В развитие указанного акцентируем внимание на позицию Н. М. Кипнис, определившего четыре критерия допустимости доказательства: «1) надлежащий субъект, правомочный проводить процессуальные действия, направленные на получение доказательств; 2) надлежащий источник фактических данных (сведений, информации), составляющих содержание доказательства; 3) надлежащее процессуальное действие, используемое для получения доказательств; 4) надлежащий порядок проведения процессуального действия (судебного или следственного), используемого как средство получения доказательств»[62]. Данная позиция ученого представляется методологически обоснованной, с точки зрения закона верной, имеющей научный и практический интерес, поскольку логически систематизирует критерии допустимости доказательства. Данные критерии применимы и к электронным уголовно-процессуальным доказательствам, поскольку последние имеют общие черты с доказательствами, закрепленными ст. 74 УПК РФ: содержание – сведения, назначение – способствуют установлению обстоятельств уголовного дела, субъект собирания – следователь, дознаватель, прокурор суд и др.

В современной теории уголовно-процессуального права особое внимание уделяется критерию «надлежащий субъект доказывания» применительно к электронным доказательствам в контексте обеспечения его допустимости.

---

[57] Балашова А. А. К вопросу о понятии «электронное доказательство» // Закон и право. 2018. №6. С.120-122.

[58] Желева О. В. К вопросу о понятии электронных доказательств и критериях допустимости их использования // Уголовная юстиция. 2021. №17. С. 44-49.

[59] Зуев С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 618-629.

[60] Гмурко В. П. Парадоксы доказательственного права // Библиотека криминалиста. 2014. № 2. С. 17.

[61] Отченаш А. Ю. К вопросу о критериях допустимости «электронных доказательств» в уголовном судопроизводстве // Вестник Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации. 2022. № 3 (95). С.80-85.

[62] Кипнис Н. М. Допустимость доказательств в уголовном судопроизводстве / отв. ред. П. А. Лупинская. М.: Юрист, 1995. С. 56.

Так, А. Е. Федулова раскрывает проблему через призму процессуальной формы электронных уголовно-процессуальных доказательств. Она указывает, что соблюдение правил их получения уполномоченными субъектами – неотъемлемый элемент допустимости. В частности, ученый выделяет следующие требования допустимости доказательств: доказательства должны изыматься и закрепляться лицами, прямо указанными в УПК РФ (следователь, дознаватель, специалист, эксперт); процессуальные документы (протоколы, заключения) должны отражать участие уполномоченных субъектов и их действия[63].

Е. И. Галяшина, развивая в своих научных трудах концепцию «цепи законных владений», уточняет, что для признания электронного доказательства допустимым необходимо установить первичного субъекта его получения, проследить маршрут передачи и хранения электронных данных, а также определить круг лиц, имевших к ним доступ. Такая фиксация обеспечивает контроль над доказательством, исключает риск его подмены или искажения и позволяет проверить законность обращения с электронными данными[64].

Таким образом, ученых объединяет идея о том, что критерий «надлежащий субъект доказывания» для обеспечения допустимости электронных доказательств предполагает: 1) обязательное участие компетентных лиц (следователя, дознавателя, специалиста, эксперта) при работе с электронными сведениями, 2) фиксацию движения электронных данных от момента их обнаружения до момента изъятия указанных данных уполномоченным субъектом.

В Постановлении Пленума Верховного Суда Российской Федерации от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской

---

[63] Федулова А. Е. Электронные доказательства в уголовном процессе: процессуальная форма и порядок получения // Закон и право. 2023. № 5. С. 45-49.

[64] Галяшина Е. И. Современные проблемы использования электронных доказательств в уголовном процессе // Вестник Московского университета МВД России. 2022. № 4. С. 67-73.

Федерации)»[65] указано, что собирание сведений о частной жизни лица, включая их закрепление техническими средствами или копирование, должно осуществляться в установленном законом порядке. Правовая позиция высшего суда обуславливает необходимость раскрытия такого критерия допустимости электронного уголовно-процессуального доказательства, как надлежащий источник доказательственной информации**.** К. А. Титова и И. В. Литвинова отмечают, что руководствоваться только традиционными критериями допустимости (без учета происхождения и возможности изменения информации) повышает риск фальсификации электронных доказательств[66]. А. И. Зазулин также рассматривает происхождение и хранение электронной информации в контексте их значимости для оценки допустимости доказательств[67].

Применительно к электронным доказательствам надлежащий источник, с которого они могут быть получены означает, что сведения должны быть получены из законного и идентифицированного носителя, к которому имелся правомерный доступ и который может быть проверен в ходе процессуальных действий. Учет данного критерия направлен на обеспечение контроля происхождения электронной информации и исключение использования сведений, полученных из незаконных или сомнительных источников информации. Конституционный Суд Российской Федерации последовательно отмечает, что сведения могут использоваться в доказывании лишь при наличии надлежащего процессуального

---

[65] Постановление Пленума Верховного Суда Российской Федерации от 25 декабря 2018 года №46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «КонсультантПлюс» (дата обращения: 04.02.2026).

[66] Титова К. А., Литвинова И. В. К вопросу о возможности применения существующих критериев допустимости доказательств к электронным доказательствам в российском уголовном процессе // Вестник криминалистики. 2023. № 4 (88). С. 45-52.

[67] Зазулин А. И. Использование электронной информации в доказывании по уголовным делам : монография. М.: Юрлитинформ, 2019. С. 68.

источника, соблюдении требований УПК РФ к способу собирания и закрепления доказательств, а также возможности их проверки в судебном заседании[68].

Согласно теории уголовно-процессуального права общим критерием допустимости электронного уголовно-процессуального доказательства выступает производство надлежащего процессуального действия, посредством которого получено электронное уголовно-процессуальное доказательство. Учет данного критерия обуславливается необходимостью процессуальной проверки достоверности перехода информации из виртуального (электронного) пространства в бумажный формат для последующего приобщения к материалам уголовного дела. Применительно к электронным доказательствам производство надлежащего процессуального действия означает, что электронные сведения должны быть получены в рамках установленного УПК РФ процессуального порядка и закреплены в соответствующем процессуальном документе (например, протоколе осмотра, обыска, выемки, осмотра электронных носителей информации и т. п.). Недостаточность только лишь «надлежащего источника» подтверждается мнениями С. В. Зуева[69] и В. Б. Вехова[70], которые справедливо отмечают онтологическую нестабильность электронных данных. Без закрепления в рамках соответствующего следственного или иного процессуального действия (например, производство осмотра согласно ст. 164.1 УПК РФ) электронная информация не приобретает свойства неизменности. Ю. В. Гаврилин акцентирует внимание на

---

[68] Определения Конституционного Суда Российской Федерации от 4 февраля 1999 года № 18-О «По жалобе граждан М. Б. Никольской и М. И. Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона «Об оперативно-розыскной деятельности»; 08 ноября 2005 года № 439-О «По жалобе граждан С. В. Бородина, В. Н. Буробина, А. В. Быковского и других на нарушение их конституционных прав статьями 7, 29, 182 и 183 Уголовно-процессуального кодекса Российской Федерации»; Постановление Конституционного Суда РФ от 16 июня 2015 года № 15-П «По делу о проверке конституционности положений статьи 139 Семейного кодекса Российской Федерации и статьи 47 Федерального закона «Об актах гражданского состояния» в связи с жалобой граждан Г. Ф. Грубич и Т. Г. Гущиной» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

[69] Зуев С. В. Электронная информация и ее носители в уголовно-процессуальном доказывании: развитие правового регулирования // Вестник ЮУрГУ. 2017. Т. 17, № 1. С. 31-35.

[70] Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография. Волгоград: Волгоградская академия МВД России, 2008.

необходимости применения специализированных программно-аппаратных комплексов и участия понятых при работе с электронными доказательствами[71].

Конституционный Суд Российской Федерации подчеркивает, что сведения, содержащиеся в электронных устройствах, средствах связи и иных цифровых источниках, могут использоваться в уголовном судопроизводстве лишь при условии их получения в рамках предусмотренного законом процессуального порядка, обеспечивающего судебный контроль, проверяемость происхождения электронной информации, возможность оценки ее достоверности и защиту конституционных прав личности. Соответственно, общим определяющим критерием допустимости электронного доказательства выступает производство надлежащего процессуального действия, посредством которого такая информация выявлена, изъята, осмотрена и закреплена[72]. Так, следователь, расследуя уголовное дело о вымогательстве, получил информацию о том, что подозреваемый хранит переписку с потерпевшим на личном ноутбуке. В установленном законе порядке следователь провел обыск по месту жительства подозреваемого, в ходе которого был изъят ноутбук. Осмотр последнего производился в присутствии понятых и специалиста по информационным технологиям. Все действия фиксировались в протоколе обыска и протоколе осмотра электронного устройства, в которых подробно указывались технические параметры, условия доступа, дата и время изъятия электронного устройства, а также были созданы электронные копии обнаруженных файлов с хэш-суммами[73]. В данном случае получение электронного доказательства осуществлялось в

---

[71] Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. №4 (44). С. 45-50.

[72] Определение Конституционного Суда Российской Федерации от 17 июля 2018 года № 1955-О «Об отказе в принятии к рассмотрению жалобы гражданина Сидака Константина Петровича на нарушение его конституционных прав частью шестой статьи 164 и статьей 177 Уголовно-процессуального кодекса Российской Федерации»; Постановление Конституционного Суда Российской Федерации от 31 марта 2011 года № 3-П «По делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами граждан С. В. Капорина, И. В. Коршуна и других» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

[73] Материалы уголовного дела № 12401460026001945. ОД УМВД России по Одинцовскому городскому округу Московской области.

рамках предусмотренного УПК РФ следственного действия – обыска с фиксацией его хода и результата с участием надлежащих субъектов. Приведенный порядок получения электронных сведений обеспечивает их допустимость, поскольку соблюдены требования относительно оснований, условия, порядка производства следственного действия.

Поскольку электронные уголовно-процессуальные доказательства по сущности, свойствам отличаются от классических доказательств, то следует дополнительно обратить внимание на важность соблюдения процессуальной формы получения и закрепления электронных доказательств. Значимость указанного критерия обусловлена риском изменения, исчезновения электронных сведений. Процессуальная форма выступает единственным процессуальным инструментом, позволяющим зафиксировать состояние электронных данных на момент производства следственного действия и обеспечить возможность последующей технико-криминалистической проверки достоверности электронного доказательства.

С. В. Зуев и В. Б. Вехов уточняют, что специфика формы закрепления электронных доказательств (предусмотренная, в частности, ст. 164.1 УПК РФ) носит не рекомендательный, а императивный характер. Участие специалиста, средств и блокираторов записи при копировании информации – это элементы процессуальной формы получения электронных доказательств, игнорирование которых лишает доказательство свойства допустимости, так как не позволяет исключить возможность модификации данных в процессе их изъятия, что сопряжено с нарушением закона при получении рассматриваемых доказательств[74]. По мнению П. С. Пастухова, именно строгость процессуальной формы получения электронных доказательств призвана компенсировать легкость фальсификации

[74] Основы теории электронных доказательств: монография / под ред. С. В. Зуева. М.: Юрлитинформ, 2021. С. 127; Вехов В. Б. Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2016. №4 (11). С.46-50.

электронных данных, выступая барьером против введения в процесс недостоверной информации[75].

Конституционный Суд Российской Федерации отмечает, что соблюдение установленной уголовно-процессуальным законом формы собирания, фиксации и закрепления доказательств выступает необходимой гарантией их допустимости и достоверности, а также защиты конституционных прав личности[76]. Аналогичной позиции придерживается и Верховный Суд Российской Федерации, ориентируя суды на необходимость в ходе судебного разбирательства по уголовному делу проводить проверку не только содержания файла, но и реквизитов формы его закрепления[77].

Таким образом, критерий – надлежащий порядок проведения процессуального действия, соблюдение процессуальной формы получения и закрепления электронных доказательств ориентирует властных субъектов уголовного процесса на обязательность проверки надежности источника электронных данных и неизменности содержания последних при установлении обстоятельства, имеющих значение для уголовного дела.

В уголовно-процессуальной науке отмечается, что существующая в настоящее время в уголовном процессе совокупность критериев допустимости для «неэлектронных видов доказательств», не может быть в полной мере применена к доказательствам электронным и, соответственно, не позволяет решить проблему их допустимости[78]. Также в качестве причин,

---

[75] Пастухов П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: дис. … д-ра юрид. наук. М., 2015. С. 230-245.

[76] Определение Конституционного Суда Российской Федерации от 16 декабря 2008 года № 1076-О-П «По жалобам граждан Арбузовой Елены Николаевны, Баланчуковой Александры Васильевны и других на нарушение их конституционных прав частями третьей и пятой статьи 165 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 04.02.2026).

[77] Постановление Пленума Верховного Суда Российской Федерации от 29 ноября 2016 года № 55 «О судебном приговоре» // СПС «КонсультантПлюс»; Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 13 января 2020 года по делу № 223-АПУ19-4 // СПС «КонсультантПлюс» (дата обращения: 05.01.2026).

[78] Титова К. А., Литвинова И. В. К вопросу о возможности применения существующих критериев допустимости доказательств к электронным доказательствам в российском

обусловливающих необходимость выработки дополнительных критериев допустимости электронных доказательств, ряд ученых выделяют следующие обстоятельства: во-первых, электронные доказательства являются неосязаемыми, и для их восприятия, исследования и оценки необходимы специальные технические устройства, а также участие лиц, обладающих специальными знаниями; во-вторых, такие доказательства легко подвергаются изменению или уничтожению. В связи с этим особое значение приобретает их своевременная и надлежащая фиксация[79].

Указывая на виртуальный (электронный) характер электронных доказательств, иные критерии допустимости уголовно-процессуальных доказательств предлагает выделять С. В. Зуев – аутентификация, идентификация, верифицируемость, воспроизводимость сведений[80]. Предложение С. В. Зуева, выделяющего для электронных доказательств особые критерии допустимости, представляется концептуально оправданным как попытка учесть техническую специфику электронной информации. В качестве достоинства такой классификации следует выделить акцентирование внимания на проверяемость происхождения и целостности электронных данных, возможность их воспроизведения в неизменном виде, то есть на те свойства электронного доказательства, без которых электронные сведения теряют доказательственное значение в уголовном судопроизводстве. Предложенные критерии, главным образом, обуславливают не столько допустимость в смысле, придаваемом в теории уголовно-процессуального права, сколько требование к надежности и проверяемости электронного доказательства, подтверждающих юридическую силу электронных сведений. Они не подменяют традиционных процессуальных

уголовном процессе // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 2 (91). С. 146.

[79] Бикмиев Р. Г., Бурганов Р. С. Собирание электронных доказательств в уголовном судопроизводстве // Информационное право. 2015. № 3. С. 20; Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12. № 5. С. 199-203.

[80] Зуев С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 618-629.

требований законности получения и закрепления сведений (надлежащий субъект, правомочный проводить процессуальные действия, направленные на получение электронных доказательств, порядок собирания электронных доказательств, соблюдение прав участников при собирании электронных доказательств, порядок изъятия, копирования, хранения электронных доказательств). Их целесообразно рассматривать в качестве специальных дополнительных требований, предъявляемых к процессуальной форме электронного уголовно-процессуального доказательства.

Отмеченное свидетельствует о необходимости обобщения и систематизации знаний о критериях допустимости электронных доказательств как самостоятельной категории уголовно-процессуального права. С учетом анализа позиций ученых и результатов правоприменительной практики в целях обеспечения надлежащей оценки допустимости электронных доказательств в уголовном судопроизводстве целесообразно выделить три группы специальных критериев – правовые, технические и регламентационные, которые в совокупности обеспечивают законность получения электронной информации, достоверность ее содержания, сохранность первоначального вида до момента исследования судом.

К первой группе следует отнести такие критерии, как: 1) степень ограничения прав и свобод участников уголовного судопроизводства; 2) недопустимость использования сведений в уголовно-процессуальном доказывании, полученных при нарушении закона.

Степень ограничения прав и свобод невластных субъектов уголовного процесса при собирании, закреплении, проверке и оценке электронных доказательств отражает необходимость соблюдения баланса между получения доказательственной информации по уголовному делу в целях публично значимого интереса и защитой фундаментальных прав граждан, организаций, закрепленных Конституцией Российской Федерации. Этот критерий подразумевает, что любые действия с электронными сведениями не должны нарушать право на неприкосновенность частной жизни, тайну переписки,

телефонных переговоров, почтовых, телеграфных и иных сообщений, а также право на защиту личной и семейной тайны. В определении Конституционного Суда Российской Федерации от 26.01.2017 № 204-О мобильные телефоны признаются электронными носителями информации и допускается, что в их памяти находится информация, содержащая охраняемую законом тайну. Согласно правовой позиции указанного Суда: «…в ходе производства обыска не допускается произвольное изъятие электронных носителей информации, на которых могут содержаться сведения, содержащие охраняемую законом тайну»[81].

Ряд ученых, признавая значимость указанного критерия, подчеркивает, что осмотр мобильных телефонов сопряжено с нарушением права на неприкосновенность частной жизни[82], что осмотром личной переписки в мобильном устройстве и осмотром почтово-телеграфных отправлений нарушается тайна телефонных переговоров, почтовых отправлений[83], но они вынуждены по причине необходимости установления обстоятельств совершенного преступления[84].

---

[81] Определение Конституционного Суда Российской Федерации от 26 января 2017 года № 204-О «Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 05.05.2026).

[82] Гасанов И. Т. К вопросу о получении судебного разрешения на осмотр сотовых телефонов участников уголовного процесса на досудебных стадиях // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий: сборник научных статей /отв. ред. С. И. Давыдов, В. В. Поляков. Барнаул, 2018. Вып. XV. С. 72-79; Иванов В. В. Защита охраняемых законом тайн при производстве следственных действий с мобильным телефоном и иными электронными носителями информации // Правовое государство: теория и практика. 2021. № 4 (66). С. 185-186; Облаков А. А. Цифровые доказательства в уголовном процессе: проблемы сбора и оценки // Закон и власть. 2024. № 5. С. 156.

[83] Токарева Е. В., Хоршева В. С. Осмотр электронных сообщений: правовая регламентация и особенности производства // Уголовное судопроизводство России: проблемы и перспективы развития: материалы всероссийской науч.-практ. конф. Санкт-Петербург, 22 ноября 2019 года. СПб, 2019. С. 348-353; Третьякова Е. И. Мобильный телефон как источник криминалистически значимой информации // Вестник Уральского финансово--юридического института. 2018. № 3 (13). С. 49-51.

[84] Архипова Н. А. К вопросу об использовании возможностей средств мобильной связи в раскрытии и расследовании преступлений // Сборник материалов криминалистических чтений. Барнаул. 2014. № 10. С. 16; Грачев С. А. Конституционные права личности при осмотре мобильного устройства: коллизия толкований в правовых позициях высших судебных

Необходимость учета степени ограничения прав и свобод невластных субъектов уголовного процесса при собирании, закреплении, проверке и оценке электронных доказательств обусловлена правовыми позициями Конституционного Суда Российской Федерации [85], в соответствии с которыми вмешательство государства в сферу частной жизни, личной и семейной тайны, а также в тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений допустимо лишь при наличии законного основания, конституционно значимой цели и при соблюдении требований необходимости, соразмерности и процессуальной гарантированности. Указанный подход приобретает особую значимость применительно к электронным доказательствам, поскольку их получение и исследование нередко сопряжены с доступом к значительному объему электронных сведений, затрагивающих не только интересы подозреваемого или обвиняемого, но и права иных лиц, не имеющих собственного интереса в уголовном деле. В связи с этим степень ограничения их прав и свобод должна рассматриваться в качестве самостоятельного критерия допустимости и надлежащего процессуального обращения с электронными доказательствами, обеспечивающего баланс между публичными интересами раскрытия и расследования преступлений и конституционной обязанностью государства по защите фундаментальных прав человека и гражданина.

Вторым правовым критерием допустимости электронного доказательства выступает недопустимость использования в уголовно-процессуальном доказывании сведений, полученных при нарушении закона. Конституционную основу рассматриваемого критерия допустимости электронного доказательства образуют предписания ч. 2 ст. 50 Конституции РФ, согласно которой при

инстанций России требует законодательного разрешения // Вестник Восточно-Сибирского института МВД России. 2020. № 3 (94). С. 139;

[85] Постановления Конституционного Суда Российской Федерации от 31 марта 2011 года № 3-П «По делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами граждан С.В. Капорина, И.В. Коршуна и других»; от 17 декабря 2015 года № 33-П «По делу о проверке конституционности пункта 7 части второй статьи 29, части четвертой статьи 165 и части первой статьи 182 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой граждан А. В. Баляна, М. С. Дзюбы и других» // СПС «КонсультантПлюс» (дата обращения: 05.05.2026).

осуществлении правосудия не допускается использование доказательств, полученных с нарушением федерального закона. В отношении электронных доказательств данное положение действует во взаимосвязи с предписаниями ст. ст. 23, 24 Конституции РФ. В уголовно-процессуальном законе содержание данного критерия допустимости электронного доказательства раскрывается прежде всего в ст. ст. 7, 74 и 75 УПК РФ, из которых следует, что доказательствами могут признаваться только сведения, полученные надлежащим субъектом, из предусмотренного законом источника и в установленной процессуальной форме

Применительно к электронным доказательствам нарушение закона может выражаться в нескольких формах: незаконный доступ к электронным сведения; не осуществление судебного контроля в случаях, когда он обязателен; подмена одного следственного действия другим; ненадлежащая фиксация электронного носителя информации и порядка извлечения электронных данных; ненадлежащее процессуальное оформление, лишающее сторону защиты возможности проверить происхождение, полноту и неизменность электронных сведений. Следовательно, вопрос о допустимости электронного доказательства должен решаться с учетом не только его содержания, но и всей процедуры его получения, исследования и приобщения к материалам уголовного дела. Анализируя положения Постановления Пленума Верховного Суда Российской Федерации от 31.10.1995 № 8[86], В. С. Ганага приходит к выводу о том, что недостаточная правовая регламентация собирания и закрепления доказательства может служить основанием для признания полученного доказательства недопустимым[87].

Правовые позиции Конституционного Суда Российской Федерации подтверждают, что сведения, затрагивающие сферу коммуникации и частной жизни лица, могут быть получены только при строгом соблюдении требований

[86] Постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 года № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

[87] Ганага В. С. К вопросу о допустимости цифровых доказательств в уголовном процессе // Санкт-Петербургские встречи молодых ученых: Материалы II всероссийского конгресса. Санкт-Петербург, 2024. С. 524.

закона. Так, Конституционный Суд Российской Федерации в Определении от 02.10.2003 № 345-О указал на конституционную охрану тайны телефонных переговоров и иных сообщений[88]. В Определениях от 09.06.2005 № 248-О[89], от 28.06.2012 № 1253-О[90] Конституционным Судом Российской Федерации уточнено, что сведения о соединениях между абонентами также относятся к сфере защиты тайны связи, а значит, их получение допустимо лишь в порядке, установленном законом. Из этого следует, что нарушение порядка получения электронных данных, связанных с перепиской, звонками и иными коммуникациями, может повлечь признание доказательств, содержание которых составляют такие данные, недопустимыми.

Позиция Верховного Суда Российской Федерации конкретизирует обозначенное требование применительно к уголовному судопроизводству. В Постановлении Пленума Верховного Суда Российской Федерации от 31.10.1995 № 8 уточнена обязанность судов исходить из конституционного запрета использования доказательств, полученных с нарушением закона[91]. В Постановлении Пленума Верховного Суда Российской Федерации от 01.06.2017 № 19 акцентировано внимание на значение судебного контроля при производстве действий, ограничивающих конституционные права граждан[92].

---

[88] Определение Конституционного Суда Российской Федерации от 02 октября 2003 года № 345-О «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» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

[89] Определение Конституционного Суда Российской Федерации от 09 июня 2005 года № 248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

[90] Определение Конституционного Суда Российской Федерации от 28 июня 2012 года № 1253-О «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

[91] Постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 года № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

[92] Постановление Пленума Верховного Суда Российской Федерации от 01 июня 2017 года № 19 «О практике рассмотрения судами ходатайств о производстве следственных

В свою очередь, Постановления Пленума Верховного Суда Российской Федерации от 29.11.2016 № 55[93], от 30.06.2015 № 29[94] ориентируют суды на использование лишь допустимых доказательств и на обеспечение стороне защиты реальной возможности проверять порядок их получения и содержание.

Одним из наиболее распространенных нарушений при собирании и процессуальном закреплении электронных доказательств является несоблюдение установленной процедуры изъятия, фиксации и сохранения исходных электронных носителей. В следственной практике нередко изымается не сам электронный носитель информации, а лишь содержащиеся на нем данные, которые копируются на сторонний электронный носитель информации. Между тем подобный подход способен существенно ограничить реализацию права стороны защиты на проверку достоверности, целостности и аутентичности электронных данных, в том числе посредством назначения повторной либо дополнительной судебной экспертизы. Отсутствие первоначального электронного носителя информации фактически исключает возможность последующего экспертного исследования его технических характеристик, структуры хранения данных, метаданных, а также установления условий создания, изменения или копирования соответствующей электронной информации. В судебной практике данное нарушение может повлечь признание таких электронных сведений недопустимыми доказательствами. Так, по одному из уголовных дел о мошенничестве суд признал недопустимым доказательством скопированные файлы, поскольку исходный жесткий диск не был изъят, что лишило сторону защиты возможности инициировать повторное экспертное исследование[95]

действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

[93] Постановление Пленума Верховного Суда Российской Федерации от 29 ноября 2016 года № 55 «О судебном приговоре» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

[94] Постановление Пленума Верховного Суда Российской Федерации от 30 июня 2015 года № 29 «О практике применения судами законодательства, обеспечивающего право на защиту в уголовном судопроизводстве» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

[95] Апелляционное определение Московского городского суда от 12 марта 2021 года по делу № 10 1234/2021// «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 06.06.2026).

Таким образом, недопустимость использования электронных сведений, полученных при нарушении закона, представляет собой самостоятельный правовой критерий допустимости электронного доказательства. Его содержание состоит в том, что электронные сведения не могут использоваться в доказывании, если они получены с нарушением конституционных прав личности, вне надлежащей процессуальной формы, в отсутствии судебного контроля либо без обеспечения проверяемости их происхождения и целостности. Следовательно, в уголовном процессе допустимость электронного доказательства определяется не только самим фактом существования электронных данных, а прежде всего законностью процедуры их получения и закрепления.

Самостоятельную группу специальных критериев допустимости электронных доказательств образуют технические критерии. Они представляют собой совокупность условий и признаков технического характера, посредством которых обеспечиваются подлинность, неизменность электронных сведений, используемых в уголовно-процессуальном доказывании. Назначение технических критериев состоит в обеспечении надежности, воспроизводимости и подтверждаемости электронных сведений. Их учет гарантирует, что представленные электронные данные действительно отражают исследуемые обстоятельства уголовного дела, не подвергались изменению и могут быть проверены специалистами, вовлекаемыми в уголовное судопроизводство.

Первостепенным техническим критерием выступает аутентичность электронного доказательства**.** Содержание данного критерия предполагает установление тождественности электронного доказательства исходным электронным данным, отсутствие несанкционированных изменений в его содержании и подтверждение легитимного источника происхождения. В уголовно-процессуальной науке на категорию аутентичности электронных доказательств обращает внимание ряд ученых. В частности, по мнению А. А. Облакова, одной из главных проблем, возникающих на этапе оценивания, выступает проверка аутентичности рассматриваемого доказательства. Она ставится под сомнение,

если данные были изменены, удалены, искажены[96]. С. В. Зуев подчеркивает роль аутентичности в обеспечении процессуальной надежности доказательств[97]. Также А. А. Шильникова указывает на необходимость аутентификации электронного доказательства[98]. П. С. Пастухов акцентирует внимание на обязанности стороны, представляющей электронные доказательства, подтвердить их целостность и неизменность. По его мнению, аутентичность выступает гарантией отсутствия фальсификации на всех этапах обращения с данными[99]. А. Е. Федулова связывает аутентичность с необходимостью придания электронным доказательствам процессуальной формы, что предполагает документальное подтверждение их происхождения и неизменности[100]. А. А. Балашова рассматривает данный критерий в качестве возможности достоверного установления источника ее происхождения[101]. По такому же принципу формируется судебная практика.

В частности, в Апелляционном определении Верховного Суда Российской Федерации от 27.12.2017 по делу № 5-АПУ17-117 предметом судебной оценки являлись снимки экрана, на которых были зафиксированы обстоятельства разбойного нападения, включая момент использования оружия в отношении потерпевшей. Данный судебное решение подтверждает, что скриншоты могут признаваться надлежащими доказательствами в уголовном судопроизводстве при условии соблюдения порядка их получения, истребования и представления, установленного ст. 86 УПК РФ. Тем самым обеспечивается возможность проверки происхождения такого доказательства, его целостности и неизменности, что имеет

---

[96] Облаков А. А. Цифровые доказательства в уголовном процессе: проблемы сбора и оценки // Закон и власть. 2024. № 5. С. 157.

[97] Зуев С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 618-629.

[98] Шильникова А. А. Электронные доказательства в уголовном процессе: понятие и критерии допустимости их использования // Проблемы права: теория и практика. 2022. № 60. С. 298.

[99] Пастухов П. С. «Электронные доказательства» в нормативной системе уголовно-процессуальных доказательств // Пермский юридический альманах. 2019. № 2. С. 695-707.

[100] Федулова А. Е. Электронные носители информации в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2022. № 2. С.90-100.

[101] Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. ... канд. юрид. наук. М., 2020. С. 14.

принципиальное значение для вывода о его аутентичности и, как следствие, допустимости в процессе доказывания[102].

Вторым техническим критерием допустимости электронного доказательства является его идентификация, заключающаяся в установлении принадлежности электронного доказательства конкретному лицу, учетной записи, устройству или информационной системе. Критерий идентификации применительно к электронному доказательству необходим по той причине, что ключевая проблема доказывания посредством электронных доказательств состоит не столько в проверке, оценке данных, касающихся обстоятельств уголовного дела, сколько в установлении того, где они обнаружены: какое устройство, какая учетная запись, какой пользователь, какая информационная система, а также какому событию во времени они соответствуют. Без идентификации электронные данные остаются неопределенными сведениями, а их доказательственное значение становится предположительным, что не согласуется с требованиями презумпции невиновности.

А. А. Шильникова обращает внимание на проблему идентификации автора электронного документа, которая заключается в необходимости достоверного установления того, что данный документ действительно исходит от лица, указанного в нем в качестве отправителя[103]. Т. М. Куценко и В. В. Здольник определяют идентификацию электронного доказательства как процесс установления его принадлежности к конкретным процессам и целям использования. Они подчеркивают, что без идентификации невозможно доказать происхождение и неизменность информации[104]. О. В. Рябова акцентирует внимание на необходимость фиксации идентификационных признаков

---

[102] Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 27 декабря 2017 года по делу № 5-АПУ17-117 // СПС «КонсультантПлюс» (дата обращения: 05.05.2026).

[103] Шильникова А. А. Электронные доказательства в уголовном процессе: понятие и критерии допустимости их использования // Проблемы права: теория и практика. 2022. № 60. С. 298.

[104] Куценко Т. М., Здольник В. В. Электронные документы как современный вид доказательств по делу об административном правонарушении // Вестник Московского университета МВД России. 2014. № 6. С. 195-202

электронных доказательств, включая метаданные (время создания файла, автор создания файла, устройство фиксации файла), контрольные суммы (хеш-значения), электронные подписи[105]. В. Ф. Васюков, С. В. Расторопов, Д. Ф. Флоря отмечают, что «в процессе раскрытия и расследования преступлений для субъекта расследования представляет неоценимое значение информация об активности в сети сотовой связи пользователя мобильного устройства, идентификация которого происходит посредством рабочего модуля SIM»[106]. «Содержанием процесса идентификации информации об абонентских соединениях является взаимодействие средств электросвязи. Результат отражения указанной идентификации представляет собой такую связь процессов взаимодействия этих средств (отражаемое) и сохранения параметров этого взаимодействия (отражение), при которой свойства первого из них (время, место, абонентские и идентификационные номера) закономерно отражаются в специфических свойствах второго (соответствующие электронные протоколы в блоках памяти)»[107]. Аналогичные правила идентификации электронных доказательств при их использовании в доказывании отражаются в правовой позиции и решениях Верховного Суда Российской Федерации. Так, в постановлении Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 уточняется, что скриншоты интернет-страниц признаются допустимыми доказательствами при условии его заверения лицом, участвующим в деле, указания URL-адреса, фиксации даты и времени получения информации[108]. В Кассационном Определении Верховного Суда Российской Федерации от

---

[105] Рябова О. В. Значение института «электронных доказательств» в отечественном уголовном судопроизводстве // Мировые исследования в области социально-гуманитарных наук: материалы III Междунар. науч.-практ. конф. Рязань, 2023. С. 374-377.

[106] Васюков В. Ф., Расторопов С. В., Флоря Д. Ф. Получение и использование абонентской информации при расследовании преступлений: Монография. Орел: Картуш, 2025. С. 73.

[107] Шампаров А. В. Механизм следообразования информации о соединениях между абонентами и (или) абонентскими устройствами // Вестник Удмуртского университета. серия экономика и право. 2014. № 4. С. 203.

[108] Постановление Пленума Верховного Суда Российской Федерации от 23 апреля 2019 года № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

07.02.2023 по делу № 5-КГ22-144-К2 указано, что скриншоты переписки признаются допустимыми доказательствами при условии наличия идентифицирующих реквизитов: адреса интернет-страницы, даты и времени фиксации, а также отсутствия заявлений о фальсификации[109].

Третьим техническим критерием допустимости электронного доказательства выступает целостность (неизменность) электронных сведений**,** предполагающая сохранение исходного состояния электронных сведений с момента их создания (фиксации) до момента представления следователю, дознавателю, суду, а также неизменность электронных сведений на всех этапах обращения с ними (изъятие, копирование, хранение, передача). Данный критерий обеспечивает подлинность электронного доказательства, исключает использование искаженных, подмененных или искусственно созданных электронных сведений. Его соблюдение – необходимое условие признания электронного доказательства допустимым в соответствии со ст. 75 УПК РФ.

В отечественной теории уголовного процесса проблема обеспечения целостности электронных доказательств исследуется Р. И. Оконенко, который включает целостность в число юридически значимых признаков электронных доказательств. По его мнению, это свойство обеспечивает соответствие электронных сведений их исходному состоянию, исключение возможности фальсификации, прослеживаемость изменений (при их наличии)[110]. А. Е. Федулова подчеркивает, что для признания электронного доказательства допустимым в уголовном процессе необходимо подтвердить сохранность его структуры и содержания с момента создания до момента представления в суд. Это требует фиксации метаданных, применения криптографических методов,

---

[109] Кассационное определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 07 февраля 2023 года № 5-КГ22-144-К2 // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

[110] Оконенко Р. И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы российского права. 2015. № 3 (52). С. 120-124.

оформления всех действий с данными[111]. А. А. Балашова указывает, что целостность выражается в отсутствии изменений в составе электронной информации, содержании и свойствах[112]. Д. А. Степаненко рассматривает вышеуказанный критерий допустимости электронного доказательства в качестве состояния электронного документа, в который после его создания не вносились никакие изменения[113]. В. Б. Вехов оценивает целостность как один из основополагающих принципов работы с электронными доказательствами. Он отмечает, что ее обеспечение реализуется через технические механизмы (хэширование, электронные подписи), процессуальные гарантии (составление протокола следственных действий)[114]. В развитие данной идеи М. С. Перцев выделяет последовательные методы обеспечения целостности электронных доказательств на этапах собирания, хранения и передачи. Автор указывает, что обеспечение целостности электронных доказательств является гарантией неизменности, целостности и достоверности данных на всех этапах – собирания, хранения и передачи[115]. З. И. Харисова обоснованно акцентирует внимание на необходимости проверки целостности электронных файлов посредством фиксации хеш-сумм на каждом этапе работы с цифровым носителем. Хеш-сумма представляет собой уникальную последовательность символов заданной длины, вычисляемую на основе содержания файла с использованием специальной хеш-функции. Особое значение обозначенного механизма заключается в том, что каждому набору данных соответствует собственное хеш-значение, а любое, даже минимальное изменение содержания файла, приводит к изменению его хеш-суммы. В связи с этим, как отмечает ученый, сопоставление результатов

---

[111] Федулова А. Е. Электронные носители информации в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2022. № 2. С.90-100.

[112] Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. ...канд. юрид. наук. М., 2020. С. 14.

[113] Степаненко Д. А. Технология собирания электронно-цифровых доказательств: проблемы и рекомендации // ГлаголЪ правосудия. 2024. № 1 (35). С. 24.

[114] Вехов В. Б. Электронные доказательства: проблемы теории и практики // Правопорядок : История, теория, практика. 2016. № 4. С. 46–50.

[115] Перцев М. С. Безопасность данных и цифровые следы: обеспечение целостности электронных доказательств в уголовном процессе // Бизнес. Образование. Право. 2025. № 2 (71). С. 213.

хеширования, полученных на различных этапах обращения с электронным документом, позволяет установить, подвергался ли файл изменениям, повреждению либо иному воздействию, и, следовательно, сделать вывод о его идентичности первоначальному состоянию[116]. Данное мнение представляет интерес для уголовно-процессуальной практики при установлении фактических обстоятельств по уголовному делу.

А. И. Туршин подчеркивает, что в различных государствах на доктринальном уровне, а в ряде случаев и в законодательстве, признается возможность подтверждения целостности электронного доказательства с помощью цифровых технологий, в том числе посредством видеозаписи процесса его собирания, фиксации хеш-значения в процессуальных документах и использования электронной подписи. По мнению автора, это придает электронной информации юридически значимые реквизиты, позволяющие рассматривать ее как электронный документ и доказательство, а также подтверждать целостность и достоверность данных при их копировании и хранении[117].

Таким образом, целостность электронных доказательств – обязательный критерий их допустимости. Необходимость его учета обусловлена особыми свойствами электронных данных, включающих уязвимость к внешним воздействиям, легкость изменения.

В качестве самостоятельного технического критерия допустимости электронных доказательств следует рассматривать верифицируемость анализируемого доказательства. Она предполагает возможность независимой проверки достоверности электронного доказательства специалистами на основе воспроизводимых методик. П. С. Пастухов подчеркивает значимость свойства верифицируемости у доказательств, полученных из электронной среды. Он, в частности, отмечает необходимость перехода от традиционных процессуальных

---

[116] Харисова З. И. Проблемы и пути совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. 2025. № 2 (108). С. 122.

[117] Туршин А. И. Электронные доказательства в уголовном процессе: опыт зарубежных стран и российские перспективы // Юридические исследования. 2025. № 9. С. 9.

гарантий сохранности уголовно-процессуальных доказательств к техническим механизмам их верифицируемости, например, к использованию современных технологий проверки целостности и происхождения электронных данных[118]. Между тем А. Н. Бачило выражает сомнения относительно допустимости электронных доказательств из-за возможного изменения электронных следов, отсутствия сертифицированных методов проверки и сложности верификации метаданных[119]. В данной связи научный и практический интерес представляет правовая позиция Верховного Суда Российской Федерации, согласно которой электронная переписка подлежит судебной оценке не сама по себе, а с точки зрения возможности установить отправителя, получателя, содержание сообщений и их связь со спорным правоотношением. Такой подход, по мнению Суда, отражает требование верифицируемости электронного доказательства, то есть его доступности для независимой проверки[120].

Таким образом, признание критерия допустимости электронных доказательств в уголовном судопроизводстве – верифицируемость нацелено на обязательность проверки надежности источника электронных сведений, их целостность и соответствие исходному состоянию. Отмеченное важно для обеспечения перспективы уголовно-процессуального доказывания, учитывая уязвимость электронных данных к изменениям, исчезновению. Обозначенным выше мнением Верховного Суда Российской Федерации также подтверждается значимость проверки достоверности электронного доказательства, что определяет направление развития уголовно-процессуального законодательства.

Самостоятельным критерием допустимости электронного доказательства является воспроизводимость рассматриваемого доказательства, означающая возможность повторного получения идентичных результатов восприятия,

---

[118] Пастухов П. С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств // Седьмой Пермский конгресс ученых-юристов: Сб. науч. ст. Пермь. 2017. С. 558-566.

[119] Бачило А. Н. Достоверность электронных доказательств: проблемы верификации // Вестник цифрового права. 2019. № 3(12). С. 45-52.

[120] Определение Судебной коллегии по экономическим спорам Верховного Суда Российской Федерации от 19 декабря 2017 года № 305-ЭС17-13540 по делу № А40-250426/2016 // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

извлечения и исследования информации, содержащейся в исходных электронных данных, при аналогичных условиях**.** По мнению С. В. Зуева, воспроизводимость позволяет многократно обращаться к электронным данным без потери содержания[121]. П. С. Пастухов уточняет, что без воспроизводимости электронное доказательство превращается в «одноразовый» артефакт, не имеющий юридической силы[122]. В кассационном определении Верховного Суда Российской Федерации от 07.02.2023 № 5-КГ22-144-К2 отмечено, что переписка в мессенджерах может быть принята в качестве доказательства, если ее содержание может быть воспроизведено в судебном заседании, участники процесса имеют возможность ознакомиться с текстом, отсутствуют заявления о фальсификации. При наличии сомнений суд вправе назначить судебную экспертизу для проверки воспроизводимости сведений [123].

С учетом изложенного следует заключить, что воспроизводимость электронных доказательств – обязательный критерий их допустимости, обеспечивающий многократное обращение к данным без потери содержания информации, содержащейся в электронном доказательстве, наглядность в ходе производства следственного действия и в судебном следствии, возможность экспертного исследования. Необходимость учета данного критерия обусловлена спецификой электронных данных, включающей зависимость от материального носителя, технического устройства и программной среды, без которых доступ к таким данным, их восприятие и проверка оказываются невозможными либо затруднительными**,** возникает риск искажения при передаче. В теории уголовно-процессуального права воспроизводимость электронного доказательства рассматривается как ключевой элемент системы критериев допустимости.

---

[121] Зуев С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 618-629.

[122] Пастухов П. С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств // Седьмой Пермский конгресс ученых-юристов: сборник научных статей. Пермь. 2017. С. 558-566.

[123] Кассационное определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 07 февраля 2023 года № 5-КГ22-144-К2 // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

Не менее важен критерий допустимости – защищенность электронного доказательства от внешнего воздействия, который исключает возможность случайного или преднамеренного изменения электронных сведений в процессе их хранения, перемещения, исследования в ходе производства по уголовному делу. Потребность в учете указанного критерия обусловлена отличительными свойствами электронных доказательств, на которые ранее указывалось в диссертации. В уголовно-процессуальной науке на проблемы защищенности электронных доказательств обращается внимание С. В. Зуевым, который подчеркивает, что этот критерий исключает искажение электронных доказательств на любом этапе уголовного судопроизводства. В постановлении Пленума от 26.12.2017 № 57 Верховный Суд Российской Федерации затронул вопросы использования электронных документов в судебных процессах, указав на необходимость соблюдения требований к их защите от несанкционированного доступа[124]. Данное требование распространяется на деятельность следователя, дознавателя и суда**,** поскольку на соответствующих стадиях уголовного судопроизводства именно они обязаны обеспечивать надлежащее обращение с электронными доказательствами, их сохранность, неизменность и защиту от несанкционированного воздействия.

На основании изложенного можно заключить, что аутентичность, идентификация, целостность, проверка достоверности, воспроизводимость, защищенность образуют единую систему технических критериев допустимости электронных доказательств. Соблюдение указанных требований, предъявляемых к электронным уголовно-процессуальным доказательствам, обеспечивает их юридическую силу, способствует формированию однородной практики уголовно-процессуального доказывания с использованием электронных доказательств.

Отдельную группу специальных критерий допустимости электронных доказательств образуют регламентационные критерии, что можно заключить из

[124] Постановление Пленума Верховного Суда Российской Федерации от 26 декабря 2017 года № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

анализа уголовно-процессуальной практики и мнений ученых по исследуемому вопросу[125]. Такие критерии представляют собой совокупность организационно-правовых мер, направленных на обеспечение аутентичности, сохранности и движения электронных сведений на всех стадиях уголовного судопроизводства. Их особенность заключается в том, что они обеспечивают установление (исследование) правовых и технических критериев допустимости электронных доказательств.

Одним из ключевых регламентационных критериев допустимости электронных доказательств является обязательность регистрации всех операций с электронным доказательством на каждом этапе его обращения**.** Такая регистрация означает систематическую фиксацию всех действий, совершаемых с электронными данными на каждом этапе их обращения в уголовном судопроизводстве: от момента обнаружения и изъятия следователем, дознавателем до приобщения к материалам уголовного дела, представления суду. В данной связи отметим верность суждения Ю. А. Чича и А. В. Романова о том, что необходимо нормативно установить обязательное требование о детальном документировании всех действий с электронной информацией, включая фиксацию хеш-сумм[126].

Значение критерия заключается в обеспечении доказательственной силы электронного доказательства за счет подтверждения его неизменности, осуществления непрерывного контроля за содержанием и формой электронного доказательства, исключающих сомнения в происхождении и целостности электронных сведений; гарантировании объективного установления обстоятельств по уголовному делу.

---

[125] Газизов В. А., Подволоцкий И. Н. Меры обеспечения электронной криминалистики // Энциклопедия судебной экспертизы. 2020. № 1 (24) С. 21-28; Гришин Д. А. Информационные технологии уголовного судопроизводства. Рязань: ИП Колупаева Е.В., 2024. С. 130; Чич Ю. А., Романов А. В. Процессуальные особенности собирания электронных доказательств в социальных сетях // Вестник экономики и права. 2026. № 113. С. 259.

[126] Чич Ю. А., Романов А. В. Процессуальные особенности собирания электронных доказательств в социальных сетях // Вестник экономики и права. 2026. № 113. С. 259.

УПК РФ прямо не предусматривает обязанность регистрации операций с электронными доказательствами (данными), хотя ряд правовых норм косвенно закрепляют требования к фиксации действий с электронными доказательствами. Так, предписания ст. 164.1 УПК РФ регулируют порядок изъятия электронных носителей информации, с обязательной фиксацией условий и способов такого изъятия; предписания ст. 81 УПК РФ обязывают приобщать к уголовному делу вещественные доказательства (включая электронные носители информации) с описанием их состояния; Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»[127] устанавливает требования к фиксации действий с электронными документами. По данному поводу Верховный Суд Российской Федерации уточнил, что при оценке скриншотов как вида электронных доказательств суд должен проверять, не произошло ли изменение их содержания при копировании, а также каким образом они сохранялись, на что ранее обращалось внимание в диссертации. Тем самым для следователя, дознавателя, суда устанавливается обязанность фиксации этапов работы с электронным доказательством[128]. В деле «Юксель Ялчинкайя против Турции», рассмотренном Европейским Судом по правам человека, также подчеркивается, что отсутствие возможности проверить целостность и достоверность электронных доказательств создает проблемы для судебной системы[129]. Следует полагать, что в европейской практике уголовно-процессуального доказывания анализируемый критерий допустимости электронного доказательства учитывается правоприменителем.

Таким образом, обязательность регистрации операций с электронными данными – важный критерий обеспечения допустимости электронных доказательств в уголовном процессе. Он позволяет подтвердить целостность электронных сведений, отследить цепочку владения ими, оптимизировать случаи

---

[127] Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

[128] Постановление Пленума Верховного Суда Российской Федерации от 23 апреля 2019 года № 10 «О применении части четвертой Гражданского кодекса Российской Федерации». П. 55 // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

[129] Постановление Большой палаты ЕСПЧ от 26 сентября 2023 года по делу «Юксель Ялчинкайя против Турции» [Электронный ресурс]. URL: echr.coe.int (дата обращения: 09.02.2026).

назначения производства судебной экспертизы для определения целостности, неизменности электронного доказательства, усилить гарантии защиты от необоснованного уголовного преследования.

В качестве второго критерия допустимости электронного доказательства регламентационного характера следует определить ограничение доступа к электронным носителям электронных данных**.** С. В. Тимофеев и Р. Х. Кочесоков по данному поводу отмечают, что существует программное обеспечение, позволяющее дистанционно перепрограммировать электронное устройство до заводских настроек либо полностью удалить информацию[130]. Ограничение доступа к указанным носителям позволяет: 1) предотвратить несанкционированное вмешательство в содержащиеся на них электронные данные. Тем самым исключается возможность изменения, удаления или добавления электронных сведений после их обнаружения в рамках уголовного дела, гарантируется, что информация на носителе останется неизменной с момента изъятия до момента ее исследования в суде; 2) обеспечить соблюдение прав личности, а именно – исключить доступ к личным данным, не относящимся к уголовному делу, минимизировать ограничения конституционных прав владельца электронного носителя информации.

Содержание рассматриваемого критерия допустимости предполагает, что доступ к электронным носителям информации предоставляется только уполномоченным лицам – следователю, дознавателю, эксперту, прокурору, суду. При этом каждое обращение к электронному носителю информации указанным субъектом подлежит документальной фиксации. Кроме того, хранение электронных доказательств должно осуществляться в защищенных помещениях, оборудование надлежит опечатывать, а электронные носители информации маркировать индивидуальными идентификаторами.

---

[130] Тимофеев С. В., Кочесоков Р. Х. Перспективы совершенствования российского законодательства в области использования цифровых следов преступления // Вестник Восточно-Сибирского института МВД России. 2024. № 4 (111). С. 270.

Фиксация действий с электронными носителями информации (изъятие электронного носителя информации, копирование электронных данных, их хранение и передача) устанавливает прозрачность процесса собирания, закрепления электронных доказательств и позволяет обеспечить в рассматриваемом плане допустимость электронного доказательства. Она включает: 1) фиксацию каждого момента обращения к электронному носителю информацию. В протоколе следственного действия (например, обыска или выемки) должны быть зафиксированы время, место, участники следственного действия, технические средства, использованные для работы с электронными сведениями, а также состояние носителя до и после производства процессуальных действий и технических операций, осуществляемых в отношении него; 2) создание криминалистической копии (образа) электронных сведений, содержащихся на электронном носителе информации. Перед началом исследования электронного носителя информации специалист обязан сделать копию электронных сведений, содержащихся на электронном носителе информации, с которым будет работать, чтобы не изменять оригинал электронных сведений, содержащихся на нем. Это позволяет сохранить первоначальное состояние электронного доказательств; 3) регистрацию изменений метаданных и хэшей файлов. Фиксация контрольных сумм помогает выявить любые изменения сведений. Такое действие позволит объективно определить допустимость электронного доказательства на предварительном расследовании и в суде, минимизировать риски признания его недопустимым из-за нарушений уголовно-процессуального порядка получения.

Одним из ключевых условий допустимости электронных доказательств выступает непрерывность документальной фиксации порядка их изъятия, передачи, хранения и исследования. Любое нарушение такой фиксации создает обоснованные сомнения в неизменности электронного носителя информации и содержащейся на нем информации, поскольку позволяет стороне защиты ставить вопрос о потенциальной подмене, изменении либо ином вмешательстве в электронные данные. В подобных случаях на сторону обвинения возлагается

дополнительная обязанность по доказыванию аутентичности и целостности представленных электронных доказательств. Судебная практика подтверждает существенность данного требования. Так, в уголовном деле о незаконном обороте наркотических средств отсутствие в материалах дела акта приема-передачи изъятого ноутбука на хранение в кладовую вещественных доказательств повлекло признание недопустимыми результатов всех последующих экспертных исследований[131].

Таким образом, ограничение доступа к электронному носителю информации и фиксация всех действий с ним – это не только регламентационные меры, но и юридически значимые действия, обеспечивающие соблюдение принципа законности, защиту прав личности в уголовном процессе.

В качестве отдельного регламентационного критерия допустимости электронного доказательства следует указать использование исключительно сертифицированных программных средств при собирании, копировании и хранении электронных данных**.** Данное требование обусловлено тем, что несертифицированные программы могут изменить структуру электронных сведений, удалить метаданные или исказить информацию, тем самым поставив под сомнение законность получения или закрепления электронного доказательства. Сертифицированные программные комплексы фиксируют все действия пользователя с электронными данными, создают контрольные хэш-суммы и обеспечивают возможность проверки целостности, аутентичности и др. полученных сведений другими специалистами. Их применение гарантирует техническую правильность действий следователя, дознавателя, суда, эксперта, исключает возможность фальсификации электронных сведений при их изъятии и обработке. По данному поводу В. А. Газизов и И. Н. Подволоцкий отмечают, что технические устройства и программное обеспечение, используемые в криминалистике и уголовном судопроизводстве, обязаны проходить сертификацию. По их мнению, отсутствие сертификата делает результаты работы

[131] Приговор Ленинского районного суда г. Кирова от 14.02.2023 по делу № 1 45/2023 // ГАС «Правосудие» (дата обращения: 07.05.2026).

с данными недостоверными, что недопустимо в уголовном процессе[132]. Д. А. Гришин отмечает, что сертифицированные средства помогают защитить конфиденциальные данные от несанкционированного доступа и повысить общую безопасность сетей информационных систем[133]. УПК РФ прямо не предусматривает требование о сертификации программного обеспечения. Ряд норм данного закона опосредованно закрепляет необходимость использования надежных средств работы со сведениями (ст. 164.1 УПК РФ), а также нормы Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[134], нормативные акты ФСТЭК[135] и ФСБ[136]. В постановлении Пленума Верховного Суда Российской Федерации от 26.12.2017 № 57 указано, что при использовании электронных документов необходимо соблюдать требования к их форме, содержанию и способу получения. Прямого упоминания сертификации в этом Постановлении нет, но подразумевается, что

---

[132] Газизов В. А., Подволоцкий И. Н. Меры обеспечения электронной криминалистики // Энциклопедия судебной экспертизы. 2020. № 1 (24) С. 21-28.

[133] Гришин Д. А. Информационные технологии уголовного судопроизводства. Рязань, 2024. С. 130.

[134] Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

[135] Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; от 14 марта 2014 года № 31 Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»; от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

[136] Приказ ФСБ России от 09 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»; от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

программное обеспечение должно гарантировать достоверность и неизменность электронных данных[137].

Таким образом, регламентационные критерии допустимости электронных доказательств выполняют своего рода контрольную функцию, поскольку обеспечивают прозрачность и проверяемость действий должностных лиц органов предварительного расследования при обращении с электронными сведениями, предотвращают утрату или искажение электронных данных, создают гарантии признания доказательства допустимым. Их учет способствует соблюдению правил уголовно-процессуального доказывания с использованием электронной среды, укреплению доверия суда к представленным электронным доказательствам как к надежным носителям, имеющих значение для уголовного дела.

Специфика электронных данных (изменяемость, нематериальный характер существования, зависимость содержания от технической среды и др.) обусловливает необходимость создания процессуальных гарантий соблюдения специальных критериев допустимости уголовно-процессуальных доказательств. В качестве таких гарантий должно выступать закрепление в УПК РФ специальных требований, предъявляемых к электронным доказательствам, обеспечивающих их допустимость. Для этого необходимо статью 75 УПК РФ дополнить частью 3, устанавливающей, что электронные сведения признаются допустимыми доказательствами при условии их соответствия общим требованиям, предусмотренным частью второй статьи 75 УПК РФ, а также при установлении аутентичности, идентификации источника, целостности (неизменности), воспроизводимости, верифицируемости пути обращения электронных сведений.

На основании изложенного можно сформулировать следующие выводы.

1. Отсутствие в УПК РФ понятия допустимости электронного доказательства и специальных критериев допустимости применительно к электронным доказательствам осложняет уголовно-процессуальное доказывание

[137] Постановление Пленума Верховного Суда Российской Федерации от 26 декабря 2017 года № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

при решении вопросов о доступе к электронной переписке, осмотре электронных устройств в отсутствии судебного решения, порядке изъятия и копирования электронных сведений, обязательном участии специалиста при производстве процессуальных действий. Вследствие указанного допустимость электронного доказательства нередко в уголовно-процессуальной практике определяется формально, что обуславливает различные стандарты доказывания по уголовному делу вопреки предписаниям главы 11 УПК РФ.

2. Формирование системы критериев допустимости электронных доказательств нацелено на надлежащее определение властным субъектам уголовного судопроизводства перспектив уголовно-процессуального доказывания, установление допустимых пределов вмешательства в охраняемые законом права, интересы личности, организаций, принятие законных решений по уголовному делу.

§ 1.3. Зарубежный опыт использования электронных доказательств в уголовном судопроизводстве и перспективы его заимствования

Исследование правовой регламентации процессуальной формы использования электронных уголовно-процессуальных доказательств в зарубежных странах позволяет критически оценить отечественный опыт в данном направлении, выявить пути совершенствования российского законодательства и правоприменения. Предметом сравнительно-правового анализа использования электронных доказательств в уголовном судопроизводстве целесообразно обозначить такие узловые вопросы современного уголовного процесса, как 1) установление нормативных правил признания электронных данных в качестве уголовно-процессуального доказательства; 2) определение специальных

критериев допустимости электронного доказательства; 3) разработка процессуального порядка собирания электронных доказательств; 4) установление допустимых пределов вмешательства в частную жизнь при доступе к электронным данным; 5) обеспечение состязательности сторон в судебном разбирательстве при исследовании фактических обстоятельств с использованием электронных доказательств.

Относительно установления нормативных правил признания электронных данных в качестве уголовно-процессуального доказательства следует отметить, что в американском законодательстве электронные доказательства не выделяются в качестве отдельного источника уголовно-процессуального доказательства[138]. Центральное место в системе уголовно-процессуального доказывания США занимают правила аутентификации Federal Rules of Evidence (далее – FRE)[139]. Так, FRE 901 требует представить достаточное основание для вывода о происхождении соответствующего электронного объекта. Для субъекта, представляющего электронные доказательства, это означает необходимость представить сведения о происхождении файла / записи, способе получения электронных данных, метаданных соответствующего файла или записи, экспертное подтверждение их подлинности и целостности[140].

Иные правила признания электронных данных в качестве уголовно-процессуального доказательства закреплены законодательством ряда европейских стран. Так, в Уголовно-процессуальном кодексе Германии[141] также отсутствует самостоятельный вид доказательства, именуемый электронным доказательством. Однако это не означает, что электронные данные находятся вне сферы уголовно-

---

[138] Макарова Е. В. Роль электронных доказательств в уголовном процессе США и Российской Федерации // Инновационный потенциал развития науки в современном мире: технологии, инновации, достижения: сборник научных статей по материалам XIII Международной научно-практической конференции. Уфа, 2023. С. 62.

[139] Federal Rules of Evidence [Электронный ресурс] URL : https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence (дата обращения 21.01.2026).

[140] Сущенко С. А. Электронные доказательства в уголовном процессе США // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 1 (98). С. 230.

[141] Strafprozeßordnung [Электронный ресурс] URL : https://www.gesetze-im-internet.de/stpo/BJNR006290950.html (дата обращения 21.01.2026).

процессуального доказывания. Напротив, они вовлекаются в процесс доказывания через традиционные процессуальные формы доказательств, предусмотренные немецким уголовно-процессуальным правом. Например, содержание переписки в мессенджере, электронной почты или файла может быть исследовано как документ, если оно представлено в распечатанном виде либо в виде зафиксированного электронного носителя; сведения о способе извлечения такой информации и ее целостности могут подтверждаться показаниями специалиста или эксперта; данные, содержащиеся на компьютере, телефоне или ином устройстве, могут быть предметом судебного осмотра. Таким образом, электронные данные в немецком уголовном процессе не образуют отдельного доказательства, а получают юридическое значение в зависимости от того, в какой процессуальной форме они введены в материалы уголовного дела и исследованы судом.

Итальянское уголовно-процессуальное законодательство в части регламентации использования электронных данных в доказывании тоже характеризуется отсутствием закрепления электронного доказательства как самостоятельного вида доказательств. Электронные данные, в зависимости от способа их получения, интегрируются в самостоятельные институты доказательственного права: документальные доказательства, результаты следственных действий по обнаружению и изъятию объектов, а также результаты оперативно-следственных мер, связанных с перехватом сообщений. Ключевым нормативным основанием для признания электронных данных в качестве доказательства выступают предписания ст. 234 УПК Италии[142], допускающие признание доказательством письменные и иные документы, которые представляют факты или предметы посредством фотографии, кинематографии, фонографии либо любого иного средства. Указанное свидетельствует о включении, хоть и в ограниченном объеме, в уголовно-процессуальный закон

[142] Codice di procedura penale [Электронный ресурс] URL : https://www.studiocataldi.it/codiceprocedurapenale/codiceprocedurapenale.asp (дата обращения 21.01.2026).

Италии источников информации в целях использования при установлении фактических обстоятельств: электронный файл, электронные сообщения, журналы событий (логи), данные системного учета, записи камер наблюдения и др. Данный факт отличает рассматриваемые нормативные правила от российского опыта в данной сфере.

Иное регулирование правил признания электронных данных в качестве электронного доказательства присуще законодательству Вьетнама. В УПК Вьетнама[143] электронные данные рассматриваются в качестве самостоятельного источника доказательств (ч. 1 ст. 87 УПК Вьетнама). Их определение легализовано в ч. 1 ст. 99 УПК Вьетнама: электронные данные охватывают сигналы, буквы, числа, изображения, звук и аналогичные элементы, созданные, сохраненные, переданные или полученные посредством электронных средств[144]. Такой опыт правового регулирования имеет научно-практический интерес, поскольку позволяет разграничить электронный объект как документ и как вещественное доказательство, повышая тем самым правовую определенность при включении электронных даны в доказательственную базу по уголовному делу.

По результатам анализа законодательства США, Германии, Италии и Вьетнама следует сделать вывод, что зарубежный опыт признания электронных данных в качестве уголовно-процессуальных доказательств демонстрирует два основных подхода: использование электронных данных в рамках традиционных процессуальных форм доказывания без их выделения в самостоятельный вид доказательств и нормативное признание электронных данных в качестве самостоятельного источника доказательств. Преимуществами первого подхода является возможность адаптации электронных данных к существующей системе доказательств, а также выработка специальных правил проверки их подлинности, происхождения и целостности. Его недостаток состоит в недостаточной

[143] Criminal Procedure Code of 27 November 2015 № 101/2015/QH13 [Электронный ресурс] URL : https://www.wipo.int/wipolex/ru/legislation/details/21477 (дата обращения 21.01.2026).

[144] Чан К. Х. Электронные доказательства при расследовании преступлений, посягающих на национальную безопасность во Вьетнаме // Universum: экономика и юриспруденция. 2026. № 2-2 (136). С. 37.

определенности статуса электронных данных. Достоинством второго подхода выступает более высокая правовая определенность правовой природы электронных данных. На основании изложенного считаем целесообразным дополнить ст. 5 УПК РФ определением «электронные данные», что позволит нормативно определить их процессуальную природу, отграничить электронные данные от документов и вещественных доказательств, обеспечить единообразие их собирания, закрепления, проверки и оценки, а также повысить правовую определенность при решении вопросов об их допустимости, достоверности и доказательственном значении в уголовном судопроизводстве[145].

Для определения оптимальности условий, порядка использования электронных уголовно-процессуальных доказательств в отечественном уголовном судопроизводстве целесообразно акцентировать внимание на опыт зарубежных стран о выделении специальных критериев допустимости исследуемых доказательств. Так, в американской системе правосудия обеспечение допустимости электронных доказательств осуществляется комплексом нормативных правил, аутентификации, установления целостности и проверяемости последних. Ключевую роль здесь играют Федеральные правила доказывания, особенно правило 901 FRE, которое устанавливает требования к аутентификации доказательств. Применительно к электронным данным это предполагает подтверждение того, что конкретный файл, запись, сообщение или выгрузка электронных данных происходит из обозначенного источника происхождения и не является произвольной или неустановленной копией исходных электронных данных[146]. Для электронной сферы принципиально важны нормы, упрощающие включение электронных записей в процесс при условии выполнения критериев допустимости: а) FRE 902(13) допускает самоудостоверение записей, сгенерированных электронным процессом или системой, – при наличии сертификации; б) FRE 902(14) допускает

[145] Приложение № 1 к диссертации.

[146] Сущенко С. А. Электронные доказательства в уголовном процессе США // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 1 (98). С. 231.

самоудостоверение данных, скопированных с электронного устройства, носителя или файла, – также при наличии сертификации. Функционально FRE 902(14) работает как правовой механизм подтверждения идентичности копии данным, содержащимся в оригинальном электронном носителе или исходном файле и тем самым обеспечивает целостность электронных данных, включая контрольную проверку достоверности (в том числе через хеш-значения – технический способ удостоверения неизменности электронных данных).

В ходе уголовно-процессуального доказывания содержание электронных записей оценивается с применением правила о наилучшем доказательстве: а) FRE 1001 закрепляет определения письменных документов, записей и фотографий, включая электронные записи; б) FRE 1002 устанавливает общее требование представления оригинала записи, документа или фотографии для доказывания содержания записи соответствующей записи, документа или фотографии; в) FRE 1003 допускает использование дубликатов оригинала, если отсутствуют существенные сомнения о подлинности оригинала либо если это не приводит к несправедливости. В совокупности указанные нормы формируют более высокую степень надежности критериев допустимости электронного доказательства по сравнению с иными правилами признания электронного доказательства допустимым, присущим таким странам, как Германия и Италия.

В частности, в немецком уголовном процессе требования аутентификации, целостности и проверяемости электронных данных формируются преимущественно не посредством детализированной технической регламентации, а через систему процессуальных гарантий, обеспечивающих установление их происхождения, неизменности и возможности последующей проверки достоверности в условиях состязательного судебного разбирательства и свободной оценки доказательств судом (§ 261 УПК Германии). В этой связи надежность электронных данных обусловливается прежде всего порядком их получения, закрепления и представления, а также возможностью проверки

примененных технических средств и порядка[147]. Аутентификация электронных данных обеспечивается, с одной стороны, юридически значимым удостоверением процессуальных электронных документов посредством квалифицированной электронной подписи и использования защищенных каналов передачи (§ 32a, § 32b УПК Германии), а с другой – процессуальной фиксацией обстоятельств обнаружения, изъятия, просмотра и извлечения электронных данных, включая файлы, журналы событий, метаданные и результаты цифрового извлечения, с последующей возможностью их экспертной оценки. Существенное значение имеет также подтверждение переноса документов в электронную форму, в том числе и в судебном разбирательстве, как элемент прослеживаемости их происхождения (§§ 32e, 256 абз. 1 № 6 УПК Германии).

Требование целостности электронных данных выражается в необходимости обеспечения визуального и содержательного соответствия документа при его переводе в электронную форму в соответствии с уровнем развития техники и с обязательной фиксацией самого процесса такого переноса (§ 32e УПК Германии). Проверяемость электронных данных обеспечивается фиксацией и сохранением существенных параметров их получения, включая специальные правила документирования скрытых мер и последующего контроля (§§ 100e, 101, 101a УПК Германии), а также гарантиями доступа стороны защиты к материалам уголовного дела, электронным носителям и результатам экспертных исследований (§§ 147, 32f УПК Германии). Тем самым в уголовно-процессуальном праве Германии достоверность электронных данных обеспечивается не признанием их в качестве самостоятельного вида доказательства, а нормативным закреплением процедур, позволяющих проверить законность их получения, подлинность происхождения, целостность содержания и возможность воспроизведения в судебном разбирательстве.

---

[147] Каламов Ж. С. Правовое регулирование электронных доказательств в странах с континентальной системой права. Опыт Франции и Германии // Евразийский юридический журнал. 2021. № 4 (155). С. 318.

Определенными особенностями обладает порядок определения допустимости электронного доказательства в итальянском уголовном процессе. Аутентификация в этом государстве рассматривается как установление юридически значимой связи между электронными данными, источником их происхождения и процессуальной формой их включения в материалы уголовного дела. Указанная процессуальная форма обеспечивается соблюдением процессуальных актов: при переходе к электронной документации закон требует обеспечения аутентичности электронного документа и допускает использование цифровой или иной квалифицированной электронной подписи как средства его юридического удостоверения (ст. ст. 110, 111 УПК Италии). Аутентификация объекта доказывания обеспечивается процессуально удостоверенным происхождением электронных данных, то есть документированием источника, из которого они получены, на основании какого мотивированного решения, а также какими процессуальными действиями были обнаружены, извлечены и закреплены. Критерий целостности электронных доказательств выражается в требовании обеспечения соответствия копии электронных данных их оригиналу и сохранения неизменности электронных данных при их копировании, изъятии и хранении, что находит отражение в нормах, регулирующих изъятие электронных данных, в том числе у провайдеров, а также процессуально корректное копирование информации (ст. ст. 254-bis, 260 УПК Италии). Критерий проверяемости электронных доказательств обеспечивается составлением протокола действий по обнаружению, извлечению, копированию и хранению данных, возможностью их исследования, а также доступа стороны защиты к материалам уголовного дела и возможности признания их недопустимыми в рамках судебного разбирательства. Следовательно, итальянский подход к допустимости электронных доказательств основан на применении к ним общих критериев допустимости, дополняемых специальными требованиями к удостоверению происхождения, обеспечению целостности и процессуальной проверяемости цифровой информации.

Иная степень нормативной определенности присуща вьетнамскому уголовно-процессуальному законодательству, в котором непосредственно сформулированы критерии оценки электронных данных в целях признания их доказательством **(**ч. 3 ст. 99 УПК Вьетнама). Данная норма охватывают основные методы доказывания в условиях цифровизации: методы создания, хранения или передачи электронных данных; методы обеспечения и поддержания целостности; методы идентификации создателя обозначенных данных[148].

Предписание ч. 3 ст. 99 УПК Вьетнама закрепляют общие правила проверки электронного доказательства через установление происхождения, подтверждение неизменности (целостности) и связи электронных данных с конкретным лицом или системой. «Указанные критерии корреспондируют общепризнанным требованиям надежности электронных доказательств и определяют для суда и участников уголовного процесса юридические границы оценки электронных данных»[149]. При этом механизм реализации указанных критериев в УПК Вьетнама носит преимущественно оценочный характер и раскрывается через процессуальные способы закрепления и проверки: фиксацию действий (ч. 2 ст. 107); организацию работы с копиями как средство защиты оригинала (ч. 4 ст. 107); обеспечение сохранности (ст. 199); общие положения о проверке и оценке доказательств (ст. 108 УПК Вьетнама). В практическом плане это означает, что подтверждение аутентичности и целостности электронных данных достигается совокупностью действий: описанием состояния носителя, фиксацией процедуры копирования, соблюдением режима хранения и, при необходимости, привлечением экспертного исследования. Итоговое же значение приобретает судебная оценка надежности и допустимости[150].

---

[148] Фам Н. Х., Во С. К., Ха К. А. Электронные доказательства и принципы собирания в уголовном судопроизводстве Вьетнама // Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений: сборник научных статей по итогам работы двенадцатого круглого стола со Всероссийским и международным участием. Шахты, 2020. С. 151.

[149] Демидов Н.Н., Фам Н. Х.. Проблемы, связанные со сбором и использованием электронных доказательств в уголовном деле во Вьетнаме // Закон и право. 2021. № 1. С. 87.

[150] Фам Н. Х. Допустимость в качестве доказательства и доказательная сила электронных данных в уголовном судопроизводстве Социалистической Республики Вьетнам (СРВ) // Актуальные проблемы организации правоохранительной и правозащитной деятельности:

По результатам анализа законодательства США, Германии, Италии и Вьетнама следует заключить, что положительной стороной зарубежного опыта является выработка специальных критериев допустимости электронных доказательств, ориентированных на установление их происхождения, подтверждение целостности, проверяемость способа получения и возможность судебного контроля достоверности электронных данных. Различия между ними проявляются в степени нормативной детализации указанных требований.

Относительно процессуального порядка собирания электронных доказательств в зарубежных странах следует обратить внимание на то обстоятельство, что в США процессуальный порядок собирания электронных доказательств реализуется посредством производства обыска и выемки, а также через специальные процедуры получения доступа к электронным сообщениям и иным данным, находящимся у провайдеров электронных коммуникационных услуг и иных правообладателей, владельцев электронных данных.

Правовым основанием изъятия электронных носителей, а равно получения содержащихся на них электронных сведений, выступает судебный ордер на обыск или выемку, выдаваемый при соблюдении конституционных требований обоснованности, конкретизации предмета изъятия и пределов допустимого поиска[151]. Существенное значение на федеральном уровне имеют положения статьи 41 Federal Rules of Criminal Procedure, регламентирующие порядок выдачи и исполнения ордеров на обыск, включая особенности обращения с электронными носителями информации, копирования электронных данных и последующего их исследования. При этом процессуальная порядок состоит из двух этапов обращения с электронными доказательствами: первоначальное изъятие соответствующего носителя либо создание копии содержащихся на нем

материалы международной научно-практической конференции / отв. ред. В. Н. Яшин. Тула, 2022. С. 189.

[151] Сергеев М. С. Электронные доказательства в уголовном судопроизводстве. Опыт США // Вестник экономики, права и социологии. 2016. № 2. С. 210.

электронных данных, а затем последующий осмотр и исследование изъятой информации.

Наряду с указанным процессуальным механизмом в США действует специальное требование, закрепленное в Electronic Communications Privacy Act 1986 года, включающем в себя Stored Communications Act, Wiretap Act и Pen Register Act. Названные нормативные акты устанавливают дифференцированный процессуальный порядок доступа властными субъектами к различным категориям электронных данных. Так, получение содержания сообщений обусловлено более высоким уровнем судебного контроля, тогда как доступ к адресным и иным сопутствующим данным допускается при соблюдении менее строгих процессуальных требований. Тем самым в американском уголовном процессе проводится разграничение между содержательными данными и метаданными, имеющее принципиальное значение для определения объема судебного контроля и допустимых процессуальных средств получения доказательственной информации.

Самостоятельным процессуальным средством получения электронных сведений выступают судебные приказы, повестки и иные обязательные для исполнения требования, направляемые иным лицам, включая провайдеров и операторов электронных сервисов. Вместе с тем пределы применения указанных средств определяются как конституционными гарантиями неприкосновенности частной жизни и защиты от необоснованного вмешательства государства, так и специальными предписаниями, регулирующими условия, объем и порядок раскрытия информации[152].

Особое значение в обеспечении допустимости и достоверности электронных доказательств имеет процессуальная фиксация. В американской правоприменительной практике такие меры включают создание побитовых форензик-копий электронных носителей, вычисление контрольных хеш-значений

[152] Ряховская Я. О. Электронно-информационные технологии в уголовном процессе США // Инновации в информационных технологиях, машиностроении и автотранспорте: сборник материалов V Международной научно-практической конференции / ред.кол.: Д. М. Дубинкин (отв. ред.) [и др.]. Кемерово, 2021. С. 150.

в целях подтверждения неизменности данных, документирование цепочки хранения доказательств, фиксацию используемых технических средств, методик и версий программного обеспечения, а также установление ограниченного режима доступа к исходным носителям информации[153]. Указанные действия имеют не только технико-криминалистическое, но и доказательственное значение, поскольку формируют надлежащую основу для последующей аутентификации электронных доказательств, подтверждения их целостности и опровержения доводов стороны защиты о возможной модификации, подмене либо искусственном изменении электронной информации. Вместе с тем указанное не является уникальным для правовой системы США. В сравнительно-правовом аспекте интерес представляет опыт Италии, где собирание и закрепление электронных данных также опосредуются специальными уголовно-процессуальными механизмами, сочетающими общие следственные действия с особыми правилами обращения с информационными и телекоммуникационными системами.

В уголовно-процессуальном законодательстве Италии процесс собирания электронных данных включает несколько нормативно предусмотренных способов получения и закрепления электронной информации, к числу которых относятся: производство осмотра либо обыска, изъятие электронных носителей информации в различных процессуальных формах, а также перехват коммуникаций. Первостепенное значение в системе указанных способов имеет осмотр как процессуальная форма обнаружения и фиксации следов преступления, в том числе установленных в электронной среде. Во-первых, правовые нормы о производстве осмотра (ст. 244 УПК Италии) ориентированы на обнаружение следов преступления. При этом законодатель указывает на возможность проведения технических операций применительно к информационным и телекоммуникационным системам, одновременно возлагая на органы расследования обязанность принятия технических мер, направленных на

[153] Малов А. А. Получение электронных доказательств от иностранных юрисдикций (на примере США) // Законность. 2018. № 9 (1007). С. 57.

сохранение оригинальных электронных данных и предотвращение их изменения. Таким образом, уже на этапе фиксации обстановки преступления устанавливается обязанность сохранения электронных источников информации. Во-вторых, ст. 247 УПК Италии закрепляет специальное процессуальное основание производства обыска в отношении информационных и телекоммуникационных систем, в том числе защищенных средствами безопасности. В соответствии с частью 1-bis указанной статьи такой обыск допускается при наличии разумных оснований полагать, что в соответствующей компьютерной или телекоммуникационной системе содержатся электронные данные, электронные информация, программные компоненты[154] либо электронные следы, имеющие отношение к расследуемому преступлению. Тем самым предметом процессуального поиска в рамках данного следственного действия признаются не только материальные носители цифровой информации, но и сами электронные данные, программные средства и цифровые следы, способные иметь доказательственное значение для установления события преступления, причастности конкретного лица и иных обстоятельств, входящих в предмет доказывания по уголовному делу. Важно, что рассматриваемая норма одновременно возлагает обязанность на властных субъектов по принятию технических мер, направленных на обеспечение сохранности исходных данных и предотвращение их изменения. Указанное предписание имеет самостоятельное уголовно-процессуальное значение, поскольку ориентировано на обеспечение неизменности цифровой информации, ее последующей проверяемости и соблюдение требований надлежащего обращения с электронными доказательствами в целях подтверждения их допустимости и достоверности. В-третьих, в ст. 253 УПК Италии предусматривается мотивированное распоряжение уполномоченного органа об изъятии предметов преступления и

[154] Программные компоненты – это составные элементы программного обеспечения, обеспечивающие выполнение отдельных функций в информационной системе, компьютерном устройстве либо цифровой среде в целом.

иных относящихся к преступлению предметов, необходимых для установления фактов.

Особое значение имеет ст. 254-bis УПК Италии, регулирующая изъятие данных у поставщиков информационных и телекоммуникационных услуг. Законодатель допускает изъятие не только путем физического изъятия носителей, но и посредством копирования данных на носитель при соблюдении процедур, обеспечивающих соответствие копии оригинальным электронным данным и ее неизменяемость; одновременно на провайдера может быть возложена обязанность обеспечить сохранность и надлежащую защиты оригинальных данных[155]. Данная правовая конструкция свидетельствует о нормативно закрепленной тенденции к минимизации вмешательства в деятельность информационной инфраструктуры при одновременном обеспечении доказательственной пригодности извлекаемых данных. Предписания ст. 260 УПК Италии предусматривают копирование, при котором юридически значимым становятся два параметра электронных данных, информации или компьютерных программ: 1) соответствие копии оригинальным данным, 2) обеспечение их неизменяемости.

Самостоятельную группу средств получения электронной информации в уголовном процессе Италии образуют перехваты телефонных разговоров или коммуникаций. Нормативную основу данного института составляют ст. ст. 266-271 и 266-bis УПК Италии. При этом ст. 266 УПК Италии определяет пределы допустимости перехвата телефонных разговоров, иных форм телекоммуникаций, а также коммуникаций между лицами, включая случаи использования программно-технического средства, внедряемого в портативное электронное устройство. Предписания ст. 266-bis УПК Италии распространяют данный порядок на перехват коммуникаций, относящихся к компьютерным и телекоммуникационным системам.

---

[155] Смирнов К. А. Об «электронных» доказательствах по уголовно-процессуальному законодательству зарубежных государств // Правовая система и вызовы современности: материалы XX Международной научно-практической конференции студентов, аспирантов и молодых ученых. Уфа, 2023. С. 942.

Указанные положения устанавливают исчерпывающий круг уголовных дел, по которым допустимо применение перехвата, процессуальные предпосылки его санкционирования, порядок производства соответствующих действий, правила документирования и архивного хранения полученных материалов, а также пределы их использования в доказывании. По общему правилу разрешение на производство перехвата рассматривается судом в ходе предварительного расследования по мотивированному ходатайству прокуратуры при наличии уголовного дела и необходимости данного средства для продолжения расследования. В неотложных случаях уголовно-процессуальный закон допускает принятия мотивированного постановления прокурором с последующим судебным уведомлением в установленные сроки.

Таким образом, если в итальянском уголовно-процессуальном законодательстве акцент делается прежде всего на перехват электронных коммуникаций под контролем суда и пределах использования его результатов, то германское законодательство сосредоточено преимущественно на процессуальных механизмах обнаружения, изъятия, исследования и сохранения электронных носителей и цифровых данных как самостоятельных объектов доказывания.

В этой связи уголовно-процессуальное законодательство Германии предусматривает комплексный порядок собирания, изъятия и обеспечения сохранности объектов, имеющих значение для доказывания, который в полной мере распространяется на электронные доказательства и цифровые носители информации. В соответствии с § 94 УПК Германии предметы, способные иметь доказательственное значение для расследования, подлежат изъятию либо иному обеспечению сохранности. Если такие объекты находятся у определенного лица и не выдаются добровольно, то допускается их принудительное изъятие. Одновременно § 95 УПК Германии закрепляет обязанность лица, во владении которого находятся соответствующие предметы, предъявить и передать их по требованию компетентных органов. Применительно к электронным доказательствам данные положения охватывают как сами устройства и носители

информации, так и содержащиеся на них электронные данные, имеющие значение для установления обстоятельств уголовного дела.

Существенной гарантией законности вмешательства в частную жизнь выступает судебный контроль. Согласно § 98 УПК Германии изъятие электронных данных, как правило, осуществляется на основании судебного решения, а в случае непосредственной опасности – также по распоряжению прокуратуры или следователей с последующим судебным подтверждением[156].

Важнейшее значение для собирания электронных доказательств имеют нормы, регламентирующие производство обыска. В силу § 102 УПК Германии в отношении обвиняемого допускается обыск его жилища, иных помещений, личности и имущества, если это необходимо для его задержания либо если имеются основания полагать, что обыск приведет к обнаружению доказательств. В отношении иных лиц в § 103 УПК Германии устанавливаются более строгие условия: такой обыск возможен лишь при наличии фактических данных, позволяющих предположить нахождение искомых предметов, следов преступления или обвиняемого в конкретном месте.

Ключевое значение для доказывания с использованием электронных доказательств имеет § 110 УПК Германии, регулирующий просмотр документов и электронных носителей данных. Прокуратура и действующие по ее поручению следователи вправе осуществлять просмотр электронных носителей непосредственно на месте проведения обыска. Более того, такой просмотр может быть распространен и на электронные носители данных, территориально отделенные от обнаруженного устройства, если доступ к ним возможен с этого устройства и существует риск утраты значимых данных. При этом сведения, имеющие значение для расследования, могут быть сохранены. Данное положение свидетельствует о том, что немецкое уголовно-процессуальное право предусматривает собирание не только самого материального носителя, но и

[156] Смирнов К. А. Об «электронных» доказательствах по уголовно-процессуальному законодательству зарубежных государств // Правовая система и вызовы современности: материалы XX Международной научно-практической конференции студентов, аспирантов и молодых ученых. Уфа, 2023. С. 934.

электронную информацию, в том числе размещенную в удаленных информационных средах[157].

Научный интерес представляют положения § 95a УПК Германии об отсрочке уведомления обвиняемого и запрете на разглашение факта изъятия или требования о выдаче данных, поскольку преждевременное информирование может повлечь удаление информации, изменение доступа к ней или иное воспрепятствование расследованию. Наряду с этим § 96 и § 97 УПК Германии устанавливают пределы допустимого вмешательства, исключая или ограничивая изъятие и исследование электронных носителей информации в случаях, когда затрагиваются государственные интересы, служебная тайна или профессиональные привилегии. Таким образом, положения § 94-110 УПК Германии формируют процессуальный механизм собирания электронных доказательств, включающий обнаружение цифровых носителей, их изъятие, просмотр, доступ к удаленным данным, сохранение значимой информации и судебный контроль за законностью производства соответствующих мер. Германская правовая модель представляет особый интерес тем, что регулированием охватывается не только материальный носитель как вещь, но и цифровая информация как самостоятельный объект познания.

Схожая по направленности, хотя и имеющая собственные нормативные особенности, модель правового регулирования собирания электронных доказательств закреплена в УПК Вьетнама (ст. ст. 107, 192, 196, 199 УПК Вьетнама). Часть 1 ст. 107 УПК Вьетнама содержит требования оперативного и полного получения электронных носителей, точного описания их фактического состояния и опечатывания; при невозможности изъятия носителя допускается копирование данных с последующим хранением, включая возложение на организации обязанности обеспечить сохранность и целостность

[157] Каламов Ж. С. Актуальные проблемы действия электронных доказательств на судебной стадии уголовного судопроизводства в Российской Федерации и странах с континентальной системой права // Аграрное и земельное право. 2023. № 3 (219). С. 214.

скопированного массива[158]. Часть 2 ст. 107 УПК Вьетнама закрепляет обязательность составления протокола при получении, изъятии и копировании электронных данных. Часть 4 ст. 107 УПК Вьетнама закрепляет правило о проведении восстановления, поиска и исследовании электронных данных только по копиям, что направлено на сохранение неизменности оригинала электронного носителя и содержащейся на нем информации**.** Результаты указанных действий должны быть приведены в воспринимаемую для участников уголовного процесса форму[159]. Ст. 192 УПК Вьетнама допускает проведения обыска с целью обнаружения электронных данных при наличии оснований полагать их связь с уголовным делом; ст. 196 УПК Вьетнама регламентирует изъятие электронных носителей и данных и допускает перенос данных при невозможности изъятия; ст. 199 УПК Вьетнама усиливает требования обеспечения сохранности, устанавливая ответственность за повреждение, уничтожение, сокрытие и иные действия, нарушающие сохранность, включая нарушение пломб; ст. 223 УПК Вьетнама закрепляет специальные следственные действия по расследованию, включая тайное прослушивание и тайный сбор электронных данных.

Положения уголовно-процессуального закона Вьетнама в целом подлежат положительной оценке, поскольку они учитывает отличительные свойства электронных доказательств, содержат правила получения, копирования, исследования и обеспечения сохранности электронной информации. К числу достоинств следует отнести закрепление требований оперативного изъятия электронных носителей, точного описания их состояния, опечатывания, обязательного протоколирования, допустимости копирования электронных данных при невозможности изъятия носителя, а также проведения восстановления, поиска и исследования по копиям электронных данных, что соответствует задаче сохранения неизменности оригинала электронных данных.

---

[158] Фам Н. Х., Во С. К. Некоторые вопросы о собирании и использовании электронных данных в уголовных делах // Вопросы российской юстиции. 2021. № 16. С. 428.

[159] Нгуен Т. Б., Тью В. Х., Нгуен В. Ч. К вопросу о сборе и анализе электронных доказательств из памяти компьютера при расследовании киберпреступлений в Социалистической Республике Вьетнам (СРВ) // Universum: экономика и юриспруденция. 2024. № 4-1 (114). С. 50.

По результатам сравнительно-правового анализа законодательства США, Италии, Германии и Вьетнама следует отметить, что положительным элементом зарубежного опыта является формирование специальных процессуальных механизмов собирания электронных доказательств, предусматривающих судебный контроль либо иные формы разрешения доступа к электронным данным, дифференциацию способов получения электронной информации в зависимости от ее характера, обязательность фиксации действий с электронными носителями и электронными данными, а также принятие мер по обеспечению их сохранности, неизменности и последующей проверяемости.

Особое значение в рассматриваемом зарубежном опыте приобретает вопрос о допустимых пределах вмешательства государства в частную сферу при получении электронных данных, поскольку именно данный аспект определяет соотношение публичных интересов уголовного преследования и гарантий прав личности в условиях цифровизации уголовного судопроизводства. В этой связи показателен опыт США, где соответствующие пределы выведены прежде всего из конституционных стандартов защиты от необоснованного государственного вмешательства. Допустимые пределы вмешательства государства в частную сферу при получении электронных данных в США определяются прежде всего Fourth Amendment, запрещающей необоснованные обыски и выемки и требующей осуществления судебного контроля и разумности вмешательства в указанной сфере[160]. В условиях виртуальной среды Fourth Amendment приобретает повышенное значение в силу большого объема электронной информации: доступ к одному электронному устройству или учетной записи может раскрывать значительный массив данных, выходящий за пределы предмета расследования. Поэтому конституционно-правовой стандарт защиты частной жизни требует, чтобы вмешательство в рассматриваемую среду было юридически обосновано и

[160] Ряховская Я. О. Электронно-информационные технологии в уголовном процессе США // Инновации в информационных технологиях, машиностроении и автотранспорте: сборник материалов V Международной научно-практической конференции / ред. кол.: Д.М. Дубинкин (отв. ред.) [и др.]. Кемерово, 2021. С. 150.

ограничено конституционно-значимой целью, а ордер на обыск содержал достаточную конкретизацию предмета следственного действия.

Дополнительная регламентация допустимых пределов вмешательства государства в сферу частной жизни обеспечивается федеральными процессуальными и специальными законодательными актами, регулирующими доступ к коммуникациям пользователей и электронным данным у провайдеров. В данной связи интерес представляют своды правил: 1) 18 U.S.C. § 2703 (Stored Communications Act, SCA), определяющий регламентацию условий доступа к данным у провайдеров; 2) 18 U.S.C. § 2518 устанавливающий порядок получения судебного разрешения на перехват содержания коммуникаций с повышенными гарантиями защиты частной жизни и судебного контроля; 3) 18 U.S.C. § 3123 регулирует получение электронных данных, традиционно связываемого с иным (как правило, менее интенсивным) характером вмешательства по сравнению с перехватом контента сообщений. Тем самым американская система уголовно-процессуального регулирования выстраивает многоуровневую систему гарантий конституционных прав личности, включающей процессуальный порядок получения ордера (Rule 41 FRCP) и специальные режимы доступа к отдельным категориям данных и коммуникаций, различающихся уровнем защищенности в зависимости от характера соответствующей информации (контент, иные сведения, электронные данные у провайдеров).

В отличие от американского опыта пределы вмешательства в частную жизнь при доступе к электронным данным в немецком уголовном процессе определяются, прежде всего, принципами необходимости и соразмерности и обеспечиваются требованием получения судебного разрешения на производство обыска и выемки. Без согласия суда допускается проведение действий в случаях неотложности с последующим осуществлением судебного контроля за их законностью. Правовое регулирование основывается на градацию вмешательств в

частную жизнь в зависимости от его интенсивности[161]. При переходе к более интенсивным способам получения электронной информации усиливаются требования к обоснованию необходимости соответствующего вмешательства и временные ограничения его осуществления, что ориентирует уголовно-процессуальную практику на необходимость минимизации объема получаемой информации и пределов доступа к ней. В уголовном процессе пределами вмешательства государства при получении электронных данных выступают недопустимость необоснованного вторжения в частную жизнь, обязанность исключения из доказательственного оборота сведений, не относящихся к предмету расследования либо затрагивающих охраняемую законом частную сферу, с обязательной процессуальной фиксацией соответствующих действий, а также обеспечение охраны профессиональной тайны посредством установления запретов либо специальных условий изъятия, исследования и использования такой информации. Дополнительную конкретизацию указанные пределы получают в рамках конституционно-правового контроля, обеспечивающего соблюдение соразмерности вмешательства и поддержание баланса между интересами уголовного преследования и защитой фундаментальных прав личности в цифровой среде.

Схожий по предмету, но отличающийся по способам нормативного выражения порядок определения пределов вмешательства в частную жизнь при доступе к электронным данным сложился в итальянском уголовном процессе. В рассматриваемом уголовном процессе пределы вмешательства в частную жизнь при доступе к электронным данным в рамках обыска и выемки (изъятия) определяются совокупностью требований правовой определенности оснований вмешательства, мотивированности принимаемого решения и последующего процессуального контроля, обеспечивающих соблюдение принципа соразмерности при вторжении в информационную сферу личности. Значимым

[161] Каламов Ж. С. Правовое регулирование электронных доказательств в странах с континентальной системой права. Опыт Франции и Германии // Евразийский юридический журнал. 2021. № 4 (155). С. 318.

ограничением в рассматриваемом случае выступает необходимость наличия достаточных правовых и фактических оснований для производства обыска информационных и телекоммуникационных систем, включая системы, защищенные средствами безопасности, а также обязательность оформления соответствующего вмешательства мотивированным процессуальным решением, что обеспечивает предварительную юридическую оценку его допустимости и необходимости (ст. 247 УПК Италии).

Одновременно одним из проявлений принципа пропорциональности выступают способы получения электронной информации, которые в наименьшей степени затрагивают права и законные интересы лица. При обращении к данным, находящимся у провайдеров информационных и телекоммуникационных услуг, допускается не только физическое изъятие носителей, но и копирование данных на иной носитель при условии обеспечения соответствия копии оригиналу и ее неизменяемости, при сохранении на провайдере обязанности по хранению и защите оригинальных данных (ст. 254-bis, 260 УПК Италии). Тем самым предел допустимого вмешательства определяется не максимально возможным объемом извлекаемой электронной информации, а достижением целей уголовного судопроизводства при минимально необходимом ограничении частной сферы. Дополнительные гарантии обеспечиваются общими правилами допустимости доказательств и защиты охраняемой законом тайны: доказательства, полученные с нарушением установленных законом запретов, не подлежат использованию в доказывании (ст. 191 УПК Италии), а профессиональная тайна и конфиденциальность общения защитника с доверителем защищаются специальными ограничениями, препятствующими неконтролируемому использованию данных, полученных в результате доступа к электронным носителям и коммуникациям (ст. 103 УПК Италии). В совокупности указанные положения позволяют охарактеризовать итальянскую модель как упорядоченный механизм необходимого и юридически контролируемого вмешательства, в рамках которого пределы доступа к электронным данным определяются требованиями

мотивированности, соразмерности, сохранности и последующей проверяемости электронной информации.

Доступ к электронным данным в УПК Вьетнама обеспечивается как производством следственных действий, так и осуществлением мер расследования. В ходе следственных действий согласно УПК Вьетнама (ст. ст. 192, 196) допустимо обнаружение электронных данных при производстве обыска и последующего изъятия (выемки) соответствующих электронных носителей информации и электронных данных. Тем самым законодатель признает специфику существования электронных данных в электронной среде, где доказательственная информация может быть закреплена как через физическое изъятие устройства, так и через извлечение данных без изъятия оборудования[162]. Наряду с этим ст. 223 УПК Вьетнама закрепляет специальные следственные действия по расследованию, включая тайное прослушивание и тайное собирание электронных данных. Данная норма отражает признание цифровых каналов коммуникации как сферы, в которой получение доказательств может осуществляться негласными методами.

Доступ к одному электронному устройству информации или учетной записи аккаунта часто открывает массив электронных сведений, выходящих за пределы предмета доказывания и затрагивающих частную жизнь, тайну коммуникаций и интересы иных лиц[163]. В этом случае ст. ст. 192, 196 и 223 УПК Вьетнама определяют правовое основание и порядок доступа к электронным данным, однако эффективность гарантий пропорциональности и минимизации вмешательства в значительной мере зависит от степени конкретизация предмета

[162] Фам Н. Х. Некоторые трудности при сборе электронных доказательств в Республике Вьетнам // Материалы Весенней Международной научно-практической сессии института права: Международного круглого стола «Умные технологии правового обеспечения конкурентоспособной предпринимательской среды», Международной научно-практической конференции «Судопроизводство в Российской Федерации и за рубежом: вопросы истории и проблемы современности». 2021. С. 199.

[163] Нгуен Т. Х. Ч. Доказательства, полученные из электронных источников в уголовном судопроизводстве Вьетнама // Universum: экономика и юриспруденция. 2024. № 9 (119). С. 64.

поиска, пределов извлечения электронной информации, режима хранения и дальнейшего ее использования.

Таким образом, допускаемые пределы вмешательства в частную жизнь во Вьетнаме определяются основанием проведения следственного действия (обыск, изъятие), осуществлением специальных мер, установленным порядком закрепления электронных данных и контроля их сохранности (ст. 108 УПК Вьетнама).

По результатам сравнительно-правового анализа законодательства США, Германии, Италии и Вьетнама следует заключить, что положительным элементом зарубежного опыта является закрепление процессуального порядка доступа к электронным данным, основанного на судебном контроле, мотивированности, соразмерности вмешательства и обеспечении сохранности электронной информации. Вместе с тем его недостатки выражаются в избыточности правового регулирования либо в недостаточной определенности отдельных процедур и значительном объеме усмотрения правоприменителя. В целом зарубежный опыт свидетельствует о целесообразности сочетания четкой регламентации оснований и пределов вмешательства с эффективными гарантиями защиты частной жизни при получении электронных данных.

С учетом приведенного зарубежного опыта целесообразно предложить закрепление в УПК РФ специальной ст. 186.2, регулирующей порядок получения электронных сведений у владельца информационной системы (сервиса), поскольку действующее российское уголовно-процессуальное законодательство не содержит в достаточной степени определенной и дифференцированной процедуры истребования таких сведений, передачи и последующего процессуального оформления[164]. Введение указанной нормы направлено на достижение нескольких взаимосвязанных целей. Во-первых, оно позволит нормативно разграничить порядок получения электронных сведений в зависимости от характера запрашиваемой информации, что соответствует зарубежному опыту дифференциации доступа к контенту сообщений, иным

[164] Приложение № 1 к диссертации.

данным и сведениям, находящимся у провайдеров или владельцев информационных систем. Во-вторых, установление обязательных требований к источнику формирования выгрузки, периоду и параметрам выборки, способам подтверждения целостности и защищенности передачи обеспечит прослеживаемость происхождения электронных сведений, их неизменность и последующую проверяемость, что имеет принципиальное значение для решения вопроса об их допустимости и достоверности. В-третьих, специальное указание на необходимость судебного решения при получении содержания сообщений, переписки и иных сведений, охраняемых тайной связи, позволит закрепить в законе пределы вмешательства в частную жизнь и привести регулирование в соответствие с требованиями соразмерности и необходимости судебного контроля. Наряду с изложенным правовая регламентация порядка приобщения полученных электронных сведений к материалам уголовного дела посредством осмотра, протоколирования либо приобщения в качестве иного документа с приложением материалов, подтверждающих их происхождение и целостность, будет способствовать единообразию правоприменительной практики, снижению риска признания таких сведений недопустимым доказательством и усилению гарантий состязательности сторон при их последующей судебной проверке. Таким образом, предлагаемая ст. 186.2 УПК РФ направлена на формирование самостоятельного, процессуально определенного и проверяемого порядка получения электронных сведений у третьих лиц, обеспечивающего баланс между интересами уголовного преследования, необходимостью сохранения электронной информации и защитой конституционных прав личности

Применительно к обеспечению состязательности сторон в судебном разбирательстве при исследовании фактических обстоятельств с использованием электронных доказательств зарубежный опыт свидетельствует о нормативном закреплении процессуальных механизмов, позволяющих стороне защиты участвовать в проверке относимости, допустимости, достоверности и доказательственной силы электронной информации. В уголовном процессе США состязательность в указанной сфере обеспечивается положениями FRE 901 и FRE

902, предоставляющими стороне защиты возможность оспаривать достаточность аутентификации электронных доказательств, происхождение электронного файла, записи или сообщения, а также надежность сертификации и системы, в которой сформированы соответствующие данные; положениями FRE 1001-1003[165], допускающими постановку вопроса о необходимости представления оригинала электронных данных либо о недопустимости использования их дубликата при наличии сомнений в подлинности или риска несправедливости; конституционно-правовыми и процессуальными механизмами судебного контроля законности получения электронных данных, вытекающими из Fourth Amendment, Rule 41 Federal Rules of Criminal Procedure, 18 U.S.C. § 2518, 18 U.S.C. § 2703 и 18 U.S.C. § 3123. Тем самым в американском уголовном процессе электронные доказательства становятся объектом проверки с участием сторон – их содержание и формы, а также законность способа получения рассматриваемых доказательств.

В уголовном процессе Италии обеспечение состязательности при исследовании электронных данных достигается посредством распространения на них общих правил судебного исследования доказательств и процессуальных гарантий оспаривания способов их получения. Основополагающее значение в данном случае имеет ст. 190 УПК Италии, закрепляющая право сторон на заявление доказательств и судебную проверку их допустимости и относимости. Применительно к электронным данным данная гарантия дополняется положениями ст. 191 УПК Италии, в силу которых доказательства, полученные с нарушением установленных законом запретов, не подлежат использованию, а также ст. 103 УПК Италии, обеспечивающей охрану профессиональной тайны и конфиденциальности общения защитника с доверителем. В сфере перехвата коммуникаций проверка электронных данных с участием сторон обеспечивается правилами ст. ст. 266-271 УПК Италии, предусматривающими судебный контроль

[165] Сущенко С. А. Электронные доказательства в уголовном процессе США // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 1 (98). С. 233.

допустимости соответствующих материалов, порядок их документирования, отбора и последующего использования в судебном разбирательстве.

В уголовном процессе Германии состязательность при исследовании электронных доказательств обеспечивается, прежде всего, гарантированным доступом стороны защиты к материалам уголовного дела и возможностью их последующей проверки в судебном заседании. Нормативную основу в данном случае составляют положения § 147 УПК Германии, закрепляющие право защитника на ознакомление с материалами уголовного дела, включая электронные носители и иные материалы, содержащие цифровую информацию, а также предписания § 32 УПК Германии, регулирующий порядок предоставления доступа к электронным материалам уголовного дела[166]. Существенное значение имеют положения § 244 УПК Германии, предусматривающие право стороны заявлять ходатайства об исследовании доказательств, в том числе о назначении экспертных исследований, направленных на проверку происхождения, целостности и достоверности электронных данных. Дополнительную гарантию обеспечивают положения § 101 абз. 7 УПК Германии, предоставляющие заинтересованному лицу право судебной проверки законности негласных мер после получения уведомления об их применении. В совокупности указанные нормы обеспечивают стороне защиты возможность оспаривать как содержание электронных данных, так и законность порядка их получения и введения в процесс.

В уголовном процессе Вьетнама обеспечение состязательности при использовании электронных доказательств связано с признанием за стороной защиты права участвовать в представлении и проверке электронной информации. Важнейшее значение в этом отношении имеет ст. 88 УПК Вьетнама, согласно которой защитник вправе запрашивать документы, предметы и электронные данные, имеющие значение для защиты, а представленные материалы подлежат

[166] Смирнов К. А. Об «электронных» доказательствах по уголовно-процессуальному законодательству зарубежных государств // Правовая система и вызовы современности: материалы XX Международной научно-практической конференции студентов, аспирантов и молодых ученых. Уфа, 2023. С. 943.

принятию, протоколированию, проверке и оценке в установленном законом порядке[167]. Соответствующая обязанность процессуального оформления закреплена в ч. 4 ст. 88 УПК Вьетнама. Кроме того, общие правила проверки и оценки доказательств, включая электронные данные, предусмотрены ст. 108 УПК Вьетнама, а критерии их доказательственного значения сформулированы в ст. 99 УПК Вьетнама. Тем самым вьетнамское законодательство закрепляет нормативную основу для участия стороны защиты в исследовании фактических обстоятельств дела с использованием электронных данных, хотя степень практической реализации данных гарантий в значительной мере зависит от детализации порядка исполнения соответствующих запросов и предоставления доступа к электронной информации[168].

Таким образом, зарубежный опыт показывает, что обеспечение состязательности в судебном разбирательстве при использовании электронных доказательств достигается посредством закрепления права стороны защиты на доступ к электронной информации, оспаривание допустимости и достоверности электронных доказательств, заявление ходатайств о дополнительной проверке последних, а также инициирование судебного контроля законности получения и использования электронных данных. Именно совокупность указанных процессуальных гарантий обеспечивает возможность объективного исследования фактических обстоятельств дела в условиях цифровизации уголовного судопроизводства.

С учетом приведенного зарубежного опыта целесообразно предусмотреть в ч. 6 ст. 164.1 УПК РФ положение, согласно которому стороне защиты обеспечивается право на получение копий электронных доказательств в форме, пригодной для их последующей проверки, исследования и оспаривания, включая предоставление электронной копии, контрольных хеш-значений, описания способа и параметров создания образа, а также сведений о ходе извлечения

---

[167] Фам Н. Х. К вопросу применения электронных данных в уголовном судопроизводстве Вьетнама // Вопросы российской юстиции. 2023. № 27. С. 607.

[168] Фам Н. Х., Во С. К. Некоторые вопросы о собирании и использовании электронных данных в уголовных делах // Вопросы российской юстиции. 2021. № 16. С. 427.

данных и примененных технических средствах, если предоставление таких материалов не создает реальной угрозы правам и законным интересам иных лиц, сохранности охраняемой законом тайны либо безопасности участников уголовного судопроизводства. Ограничение указанного права должно допускаться только на основании мотивированного процессуального решения с обеспечением возможности его судебного обжалования. Закрепление такого правила направлено на усиление состязательности сторон, поскольку обеспечивает стороне защиты реальную возможность проверки аутентичности, целостности, происхождения и истории получения электронных данных, а следовательно, и полноценного оспаривания их допустимости и достоверности в судебном разбирательстве.

Проведенный сравнительно-правовой анализ правового регулирования использования электронных доказательств в уголовном судопроизводстве США, Германии, Италии и Вьетнама позволяет сформулировать ряд выводов.

1. Для каждой зарубежной правовой модели использования электронных доказательств в уголовном процессе присущи особенности, обусловленные отличительными правовыми системами, национальными традициями, представляющие интерес для оптимизации российского уголовного судопроизводства.

В большинстве рассмотренных стран (исключение – Вьетнам) электронные доказательства не выделяются как особый вид доказательства в системе доказательств. Наибольшую нормативную определенность демонстрирует вьетнамская правовая модель, закрепляющая электронные данные в качестве самостоятельного источника доказательств и устанавливающая процессуальные требования к их получению, копированию и исследованию преимущественно по копиям электронных данных, что минимизирует риск изменения оригинала электронных данных.

Американское уголовно-процессуальное законодательство закрепляет значимые гарантии допустимости электронных доказательств, выражающиеся в нормативной регламентации их аутентификации, а также в установлении условий

использования оригиналов и дубликатов электронных данных, что ориентировано на подтверждение происхождения электронных данных и их неизменности.

Итальянское уголовно-процессуальное регулирование направлено на обеспечение целостности электронных доказательств, при котором правовое значение придается процессуально надлежащему копированию электронной информации, а также допустимости получения электронных данных у провайдеров при соблюдении требований соразмерности вмешательства и минимизации воздействия на информационную инфраструктуру.

Немецкая модель правового регулирования демонстрирует, что надежность электронных данных обеспечивается совокупностью процессуальных гарантий, направленных на контролируемость порядка их получения, фиксации и исследования в условиях свободной оценки электронных доказательств судом, включая гарантии доступа стороны защиты к материалам уголовного дела и последующего судебного контроля за применением скрытых мер по получению электронных данных.

3. В зарубежных странах доказательственное значение электронных данных в уголовном судопроизводстве обусловливается не их электронной формой, а соблюдением процессуальных условий их собирания, фиксации, сохранения и проверки. К числу таких условий относятся: 1) наличие прослеживаемой истории получения электронных данных, обеспечиваемой фиксацией соответствующих действий, документированием порядка хранения и фиксацией параметров извлечения электронной информации; 2) соблюдение требований необходимости и соразмерности вмешательства в частную жизнь, включая конкретизацию пределов поиска, минимизацию объема извлекаемых электронных сведений; 3) обеспечение состязательности сторон, предполагающей предоставление стороне защиты доступа к электронным сведениям и процессуальных возможностей оспаривания происхождения, аутентичности, целостности и доказательственного значения электронных данных.

Глава 2. Обеспечение юридической силы электронных доказательств в ходе предварительного расследования

§ 2.1. Собирание электронных доказательств субъектом расследования: правовое регулирование, особенности процессуального порядка

Относительно понимания собирания уголовно-процессуальных доказательств в науке уголовного процесса существуют различные точки зрения. По мнению С. А. Шейфера, под собиранием доказательств следует понимать «систему действий, обеспечивающих восприятие субъектом доказывания объективно существующих следов изучаемого события, сопровождающихся формированием в сознании познавательного образа, а также действий, обеспечивающих сохранение этого образа, путем процессуальной фиксации результатов восприятия»[169]. С. А. Шейфер акцентирует внимание на познавательном и процессуальном аспектах собирания доказательств. Это важно, поскольку доказывание начинается с осознания и понимания властным субъектом фактов, связанных с изучаемым событием, а также их отражения в сознании этого субъекта. Акцент ученого на процессуальный характер обозначенной деятельности, определяемый необходимостью фиксации результатов осознания, понимания, отражения в сознании, подлежит учету в уголовно-процессуальной деятельности.

С. Б. Россинский иначе представляет процесс собирания доказательств, предлагая, в отличие от традиционного понимания, первый элемент процесса доказывания рассматривать шире. По мнению указанного ученого, собирание

[169] Шейфер С. А. Собирание доказательств в советском уголовном процессе. Методологические и правовые проблемы. Саратов: Изд-во Саратовского ун-та, 1986. С. 24.

доказательств – это комплекс предусмотренных законом приемов и процессов, посредством которых в досудебное или судебное производство вводятся любые предметы, документы и сведения, обладающие познавательной ценностью, и который завершается их процессуальным оформлением, то есть легализацией и приданием им необходимой юридической силы[170]. С. Б. Россинский в данном случае подчеркивает нормативную основу доказывания, а также процессуальный порядок его осуществления. Такое понимание собирания уголовно-процессуальных доказательств более восприимчив правоприменителями в уголовном судопроизводстве. Аналогичной позиции придерживались П. А. Лупинская[171], А. И. Винберг[172] и Р. С. Белкин[173], которые связывали собирание доказательств с осуществлением уполномоченными субъектами комплекса действий по обнаружению, получению, изъятию, фиксации и сохранению фактических данных. При этом отдельные исследователи, например А. О. Бестаев, фактически отождествляют собирание доказательств с их формированием, включая в это понятие выдвижение следственных версий. Представляется, что такое мнение сложно поддержать, поскольку выдвижение следственной версии выступает самостоятельным элементом познавательной деятельности, предшествует осуществлению действий, на которые выше указывалось, и не образует самостоятельного элемента процесса собирания доказательств[174].

Таким образом, собирание уголовно-процессуальных доказательств является системообразующим элементом процесса доказывания по уголовному делу, сущность которого в юридической литературе определяется по-разному. Контент-анализ научной литературы позволяет рассматривать собирание

---

[170] Россинский С. Б. Собирание доказательств как «первый» этап доказывания по уголовному делу. Юридический вестник Самарского университета. 2020. Т. 6, № 3. С. 91-103.

[171] Лупинская П. А. Уголовно-процессуальное право: учебник. М.: Норма, 2006. С. 355.

[172] Винберг А. Й. Криминалистика : учебник для юридических вузов. Ч. 1 / под ред. А.И. Винберга. М.: Гос. изд-во юрид. лит., 1950. С. 16-17.

[173] Белкин Р. С. Собирание, исследование и оценка доказательств. Сущность и методы. М.: Наука, 1966. С. 29.

[174] Бестаев А. О. Способы собирания доказательств в уголовном процессе России : дис. ... канд. юрид. наук. Нижний Новгород, 2007 С. 229.

уголовно-процессуальных доказательств как комплекс познавательных и процессуальных действий**,** направленных на выявление, получение, восприятие и закрепление фактических данных, имеющих значение для уголовного дела, предусматривающий их последующую проверку и оценку уполномоченным субъектом.

Особенности правового регулирования собирания электронных сведений в целях доказывания по уголовному делу следует рассматривать через призму общих положений уголовно-процессуального закона о доказывании. Согласно предписаниям ст. ст. 74, 81, 84, 86, 164, 164.1, 166-167, 176-178, 182 и 183 УПК РФ процессуальный порядок собирания электронных сведений в уголовном судопроизводстве представляет собой установленную уголовно-процессуальным законом последовательность действий следователя, дознавателя, направленных на выявление источника электронной информации, извлечение указанных сведений, их последующее процессуальное закрепление и придание им статуса уголовно-процессуального доказательства.

Исходным элементом данной теоретической конструкции выступают положения ч. 1 ст. 74 УПК РФ, согласно которым доказательствами по уголовному делу признаются любые сведения о фактах, на основании которых устанавливаются обстоятельства, подлежащие доказыванию, а также иные обстоятельства, имеющих значение для уголовного дела. Электронная информация, содержащая сведения об указанных фактах, может выступать источником доказательственной информации, однако приобретает статус доказательства только при условии ее получения и закрепления в предусмотренной законом процессуальной форме.

Деятельность по собиранию доказательств в досудебном производстве, в первую очередь, регламентируется положениями ст. 86 УПК РФ, в соответствии с которыми следователь, дознаватель осуществляет собирание доказательств путем производства следственных и иных процессуальных действий. Применительно к электронным сведениям это означает, что они могут быть получены в ходе производства следователем, дознавателем следственных действий: осмотра

(ст. 176-178 УПК РФ), обыска (ст. 182 УПК РФ), выемки (ст. 183 УПК РФ), а также путем истребования документов и предметов от учреждений, предприятий, организаций, должностных лиц и граждан в порядке, предусмотренном ст. 86 УПК РФ, либо путем представления предметов и документов участниками уголовного судопроизводства. Ученые отмечают, что электронные сведения, в том числе аудио- и видеозаписи, могут возникать как в результате процессуальной деятельности органов расследования (например, при производстве следственных действий), так и в результате оперативно-розыскных мероприятий либо действий граждан, ставших свидетелями противоправных событий. В последнем случае такие материалы представляются следователю и подлежат процессуальной проверке и закреплению[175].

Следует уточнить, что правовую регламентацию процессуального порядка собирания электронных доказательств можно градировать следующим образом. Во-первых, обозначенный порядок регулируется общими предписаниями уголовно-процессуального закона о доказывании и производстве следственных действий (ст. ст. 74, 164 и др. УПК РФ), а во-вторых, – специальными нормами (ст. ст. 81.1, 164.1 УПК РФ), учитывающими сущность, особенности происхождения, формат существования электронных сведений, порядка изъятия электронных носителей информации. Указанное требует от следователя, дознавателя определенного уровня знаний в области современных информационных технологий, чтобы эффективно расследовать преступления, совершаемые в информационно-телекоммуникационной среде. Понимание принципов функционирования сетей связи, систем дистанционного банковского обслуживания, механизмов идентификации пользователей в сети Интернет и способов сокрытия цифровых следов позволяет более точно формулировать запросы о предоставлении информации, грамотно назначать производство судебных экспертиз и правильно определять круг электронных данных, имеющих

[175] Чеботарева И. Н., Лунева К. А., Рейц А. Н. Актуальные вопросы использования аудиозаписи в качестве доказательства в уголовном процессе // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2025. № 3. С. 72.

доказательственное значение для уголовного дела. На данный факт указывают Т. К. Рябинина, Я. П. Ряполова, Д. О. Чистилина[176]. В данной связи справедливо обращают внимание О. В. Химичева и П. О. Панфилов на то обстоятельство, что изменяемая в условиях цифровизации уголовно-процессуальная форма требует учета квалификации и специализации правоприменителя[177].

Системный анализ представленных выше правовых норм через призму положений теории уголовного процесса о доказывании позволяет заключить, что процессуальный порядок собирания электронных доказательств представляет собой совокупность предусмотренных уголовно-процессуальным законом действий уполномоченных субъектов, направленных на обнаружение источников электронных сведений, получение электронной информации и ее носителей, закрепление полученных электронных сведений в установленной процессуальной форме. В данной связи заслуживает внимание утверждение О. В. Химичевой о том, что расширение использования данных в электронном виде является трендом развития деятельности государственным органов[178], к которым относятся и органы предварительного расследования. В условиях электронной среды юридическая сила электронных сведений должна определяться не только содержанием информации, но и соответствующим порядком ее извлечения и закрепления, учитывающим повышенную изменяемость электронных сведений, их зависимость от программной среды, легкость копирования без внешне различимых признаков.

Анализ уголовно-процессуального законодательства и правоприменительной практики позволяет выделить пять основных способов собирания электронных

---

[176] Рябинина Т. К., Ряполова Я. П., Чистилина Д. О. Актуальные проблемы вы явления и расследования дистанционных хищений с банковского счета // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2023. № 4. С. 31-38.

[177] Химичева О. В., Панфилов П. О. Изменение уголовно-процессуальной формы в условиях цифровизации: новые риски и возможности // Вестник Московского университета МВД России. 2024. № 1. С. 161.

[178] Химичева О. В. Развитие уголовно-процессуального доказывания в условиях цифровой трансформации // В сборнике: Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности: сборник научных статей по материалам международной научно-практической конференции. М., 2023. С. 187-188.

сведений, различающихся по источнику получения информации и процессуальной форме ее закрепления: 1) изъятие электронного носителя (устройства) и последующий осмотр (исследование) электронной информации[179]; 2) копирование информации с электронного носителя (в том числе создание образа электронной информации) и приобщение копии электронной информации (или производных последней) к материалам уголовного дела[180]; 3) получение электронных сведений от иных лиц (организаций, операторов, банков, владельцев сервисов, администраторов информационных систем)[181]; 4) получение и проверка электронных сведений посредством назначения и производства судебной экспертизы; 5) легализация электронных сведений, первоначально выявленных в рамках оперативно-розыскной деятельности, путем их последующего процессуального закрепления[182]. Указанные способы нередко применяются субъектом расследования в совокупности, что усиливают юридическое значение собранных по уголовному делу электронных доказательств.

Вышеуказанные способы собирания электронных сведений через призму анализа предписаний ч. 1 ст. 86 УПК РФ позволяют представить процессуальный порядок собирания электронных доказательств как последовательность взаимосвязанных этапов, каждый из которых имеет самостоятельное значение для обеспечения юридической силы электронных сведений, имеющих значение для уголовного дела: 1) выявление источника электронных сведений и обеспечение сохранности указанных сведений; 2) выбор процессуальной формы получения

---

[179] Апелляционные определения Московского городского суда от 03 июня 2024 года по делу № 10-6860/2024; от 13 ноября 2024 года по делу № 10-22619/2024;от 28 июля 2024 года № 01-0011/2024 // «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 09.02.2026).

[180] Кассационное определение Первого кассационного суда общей юрисдикции от 27 февраля 2025 года по делу № 77-629/2025 // СПС «КонсультантПлюс» (дата обращения: 10.02.2026).

[181] Кассационные определения Первого кассационного суда общей юрисдикции от 20 мая 2025 года № 77-1553/2025; от 06 августа 2025 года № 77-2514/2025 // СПС «КонсультантПлюс» (дата обращения: 10.02.2026).

[182] Кассационное постановление Первого кассационного суда общей юрисдикции от 16 января 2024 по делу № 77-204/2024 // СПС «КонсультантПлюс» (дата обращения: 05.01.2026).

электронного носителя и электронных сведений; 3) закрепление электронных сведений в уголовном судопроизводстве.

Обнаружение источника электронных сведений является одним из проблемных вопросов в ходе собирания электронных доказательств. Данное действие, как отмечается в научной литературе, имеет принципиальное значение для определения достоверности и, соответственно, доказательственного значения последних[183]. Установление источника электронных сведений предполагает выявление механизма образования электронного следа и определение электронного носителя информации либо информационной системы, в которой соответствующие сведения были сформированы или сохранены. Источником электронных сведений могут выступать: 1) лицо, создавшее или распространившее электронную информацию (автор сообщения, отправитель файла)[184]; 2) устройства, на котором информация создана или сохранена (телефон, компьютер)[185]; 3) информационная система или сервис, на серверах которого информация хранится (социальная сеть, мессенджер, почтовый сервис)[186]; 4) инфраструктура связи, фиксирующая технические параметры коммуникаций (оператор связи, провайдер доступа в сеть Интернет, хостинг-провайдер, владелец сетевого ресурса)[187].

---

[183] Количенко А. А. О специфике проверки электронных доказательств в уголовном процессе // Альманах молодых ученых. 2022. № 2. С. 108-114.

[184] Приговор Замоскворецкого районного суда города Москвы от 20 ноября 2025 года по делу № 1-441/2025; Приговор Измайловского районного суда города Москвы от 19 марта 2026 года по делу № 1-158/2026// «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 20.04.2026).

[185] Приговор Головинского районного суда города Москвы от 13 марта 2025 года по делу № 1-001/2025; Приговор Перовского районного суда города Москвы от 13 ноября.2025 года по делу № 1-1117/2025; Приговор Таганского районного суда города Москвы от 17 апреля 2025 года по делу № 1-176/2025// Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

[186] Приговор Останкинского районного суда города Москвы от 09 декабря 2025 года по делу № 1-764/2025; Приговор Хамовнического районного суда города Москвы от 11 декабря 2023 года по делу № 1-85/2025// Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026);

[187] Приговор Нагатинского районного суда города Москвы от 13 августа 2018 года по делу № 1-419/2018// Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 21.04.2026);

В ходе предварительного расследования установление следователем, дознавателем источника электронных сведений производится как посредством процессуальных действий (изъятие, осмотр, выемка, обыск), так и путем получения информации у иных лиц. При этом важно различать получаемые результаты: установление технического источника (устройство, аккаунт, сервер, IP-адрес) и установление субъекта-источника (конкретное лицо, осуществившее создание, отправку, размещение электронной информации). Для установления фактических обстоятельств совершенного преступления это имеет принципиальное значение, поскольку ошибочное заключение следователя, дознавателя о лице, создавшем электронные сведения, приводит к неверной юридической оценке доказательства и процессуальным решениям (включая предъявление обвинения), принимаемым властным субъектом по уголовному делу. Подтверждением указанного является пример из следственной практики. В ходе расследования преступления следователь приобщил к материалам уголовного дела скриншоты переписки, полученные с телефона потерпевшего. Впоследствии не было установлено, что аккаунт использовался несколькими лицами, что потребовало проведения следователем дополнительных следственных действий, в том числе назначения судебной экспертизы, что повлияло на увеличение срока предварительного расследования, процессуальных издержек по уголовному делу[188]. Причиной указанного явилось неверное установление следователем связи между номером телефона / аккаунтом с конкретным лицом, хотя в электронной среде это не всегда осуществимо: возможны передача SIM-карты, использование иными лицами нескольких устройств, подмены аккаунта, компрометация доступа. В данной связи практические интерес имеет мнение Е. И. Галяшиной, которая в своем исследовании указывает на необходимость соблюдения принципов, закрепленных Международной организацией по компьютерным доказательствам (IOCE), при обнаружении, закреплении, изъятии и сохранении цифровых данных. Ученый подчеркивает, что важно не только

[188] Материалы уголовного дела № 1250145045000025. СО ОМВД России по району Измайлово г. Москвы.

установить технический источник, но и провести его анализ с учетом возможности использования посредников, что влияет на определение субъекта-источника[189].

Ненадлежащее установление источника электронных сведений в ходе предварительного расследования влечет существенные негативные последствия как для эффективности расследования уголовного дела, так и для обеспечения прав личности, проявляющиеся в формировании ошибочных следственных версий, утрате либо снижении доказательственного значения электронных сведений, принятии необоснованных процессуальных решений, включая незаконное предъявление обвинения в совершении преступления. Указанная проблема особенно значима в условиях, когда доступ к одному устройству, аккаунту, номеру телефона или иному идентификатору может иметь несколько лиц, а также при возможной компрометации учетных данных, передаче SIM-карты, использовании удаленного доступа, средств анонимизации и иных способов сокрытия действительного пользователя. В подобных случаях ошибочная характеристика электронных сведений сопряжена с ограничением конституционных прав личности.

В целях преодоления проблемы ненадлежащего установления источника электронных сведений в уголовном судопроизводстве и минимизации связанных с этим негативных последствий представляется необходимым совершенствование уголовно-процессуального регулирования в рассматриваемой части. Целесообразно в ст. 5 УПК РФ закрепить понятия «технический источник электронных сведений» и «субъектный источник электронных сведений»[190]. Значение такого законодательного разграничения состоит в том, что оно позволяет устранить одну из наиболее распространенных ошибок, допускаемых субъектами предварительного расследования, – необоснованный перенос акцента

[189] Галяшина Е. И. Оценка достоверности цифровых фонограмм в уголовном процессе // Доказывание и принятие решений в современном уголовном судопроизводстве: материалы Международной научно-практической конференции, посвящ. памяти докт. юрид. наук, проф. Полины Абрамовны Лупинской: сборник науч. трудов. М., 2011. С. 139.

[190] Приложение № 1 к диссертации.

исследования с признаков технической принадлежности электронной информации на создателя и пользователя электронной информации. Установление обстоятельства, что определенные сведения обнаружены в конкретном телефоне, компьютере, аккаунте либо информационной системе, не подтверждает факта, что именно определенное лицо осуществило их создание или распространение.

В УПК РФ (ст. 74) требуется также закрепить правило о приоритетном изучении полученных электронных сведений в первоначальном виде. При отсутствии такой возможности следователь, дознаватель исследует их производные формы[191]. Оно предусматривает следующий порядок действий субъекта расследования. Если получение электронных сведений из первоначального источника их формирования возможно, то изъятие и исследование рассматриваемых сведений должны осуществляться непосредственно из устройства, информационной системы, сервера, облачного хранилища, а также у оператора связи или владельца соответствующего сервиса. Использование скриншотов, распечаток, фотографий экрана и иных производных форм фиксации электронных сведений допустимо лишь, когда отсутствует возможность получения первоначальных данных. В таком случае обязательным является указание в протоколе соответствующего процессуального действия причин не использования в уголовно-процессуальном доказывании оригинального содержания электронных сведений и факта проверки достоверности представленных сведений. Закрепление в уголовно-процессуальном законе данного правила необходимо ввиду того, что производные формы электронных сведений не воспроизводят в полном объеме свойства указанных сведений, включая метаданные, сведения о времени их создания и изменения, параметры передачи и иные характеристики, имеющие значение для установления природы происхождения обозначенной информации.

Важной проблемой при собирании электронных доказательств является предотвращение уничтожения обнаруженных электронных сведений и необходимость оперативного обеспечения их сохранности. Как отмечают

[191] Приложение № 1 к диссертации.

М. Г. Янин и К. М. Кочедыкова, «электронные сведения, записанные на электронных носителях информации и имеющие значение для расследования уголовного дела, могут быть скрыты либо уничтожены»[192]. Электронные сведения легко уничтожаются посредством удаления, шифрования, дистанционной очистки, автозатирания. В ходе предварительного расследования это создает риск утраты доказательств еще до их процессуального закрепления. На данный факт обращал внимание и П. С. Пастухов[193]. В связи с этим, как отмечают ученые, особое значение приобретает своевременная фиксация таких данных и обеспечение их сохранности[194]. Указанная позиция ученых представляется обоснованной и отражает сущность электронной информации как объекта уголовно-процессуального доказывания. Исходя из изложенного, обосновано констатировать, что своевременное закрепление и обеспечение сохранности электронных сведений выступают необходимым условием их последующего эффективного использования в качестве доказательств. В противном случае возникает риск утраты значимой доказательственной информации, снижения достоверности электронного доказательства при ненадлежащем установлении источника формирования (происхождения) электронных сведений, а также невозможности подтверждения целостности и неизменности рассматриваемых данных. Отмеченное усложняет оценку допустимости и относимости соответствующих сведений, может способствовать затягиванию сроков расследования и повышению вероятности судебных ошибок в судебном разбирательстве по уголовному делу.

В целях нивелирования рисков искажения или уничтожения электронных данных, обнаруженных следователем, дознавателем и имеющих значение для уголовного дела, целесообразно в УПК РФ включить самостоятельное

---

[192] Янин М. Г., Кочедыкова К. М. Проблемы сбора, проверки и оценки электронных доказательств // Управление в современных системах. 2019. № 2. С. 29.

[193] Пастухов П. С. Цифровая криминалистика: монография. М., 2021. С. 78.

[194] Рябинина Т. К., Чистилина Д. О., Ряполова Я. П. Цифровая трансформация уголовно-процессуального доказывания: преимущества и риски // Вестник Томского государственного университета. 2025. № 516. С. 225.

следственное действие – «Безотлагательное сохранение электронных данных»[195]. Закрепленные УПК РФ процессуальные действия (истребование документов и сведений, обыск, выемка) не всегда позволяют без риска утраты, изменения обнаруженных электронных данных изъять последние в процессуально допустимой форме по причине действия временного фактора. Производство предлагаемого следственного действия позволяет оперативно сохранить электронные данные у третьих лиц (провайдеров, операторов связи, банковских учреждений и т.д.). Оно не подменяет собой процессуальное действие, указанное выше, а обеспечивает перспективу существования, целостность и проверяемость электронных данных, сохранность путей их движения и др.

Содержание анализируемого следственного действия состоит в возложении следователем, дознавателем на адресата (оператора связи, владельца информационного сервиса, организацию правообладателя электронных сведений) обязанности незамедлительно обеспечить сохранение конкретно определенного следователем, дознавателем объема электронных данных и не осуществлять их удаление, изменение или перезапись в установленный властным субъектом срок. Отличие данного следственного действия от других следственных действий, в ходе которых может быть получено электронное доказательство, заключается в том, что с его помощью обеспечивается сохранность данных на определенный срок, не предусматривающее раскрытие содержания сведений следователю, дознавателю. Последующее получение субъектом расследования уголовного дела сохраненных электронных данных осуществляется в порядке, предусмотренном УПК РФ, включая получение разрешения суда в случаях, связанных с нарушением охраняемыми законом тайнами (тайна связи, переписки и др.). Таким образом обеспечивается баланс между эффективностью доказывания обстоятельств уголовного дела (предотвращается утрата электронных данных) и соблюдением прав личности на неприкосновенность частной жизни, тайны переписки.

Необходимостью защиты законных интересов владельцев электронного устройства или владельцев электронной информации, содержащейся на указанном

[195] Приложение № 1 к диссертации.

устройстве, обусловлено участие специалиста при изъятии электронного носителя информации. В то же время, как полагают отдельные ученые, «положения уголовно-процессуального закона, обязывающие следователя привлекать специалиста, могут нарушать требования закона о процессуальной самостоятельности следователя»[196]. Согласно результатам проведенного эмпирического исследования 39 % респондентов из числа следователей, дознавателей привлекают специалиста чаще всего при необходимости копирования информации с ее электронного носителя. При этом 14 % указанных респондентов отметили необходимость безусловного привлечения специалиста в ходе отмеченного способа собирания электронных сведений. При необходимости же получения электронных сведений из облачного хранилища и с электронного носителя, к производству следственных действий специалиста привлекают соответственно 20 % и 16 % опрошенных следователей, дознавателей[197]. Иную позицию по исследуемому вопросу занимают адвокаты-защитники по уголовным делам. Треть из них отметили необходимость безусловного привлечения специалиста при собирании электронных доказательств. Порядка 20 % указанных респондентов считает целесообразным привлечение специалиста в зависимости от ситуации: при копировании с электронного носителя информации, при изъятии электронных сведений из облачного хранилища, содержащихся на электронном носителе информации[198].

Представляется, что участие специалиста требуется не во всех случаях изъятия электронного носителя, а в так называемых трудных процессуальных ситуациях, когда без специальных знаний существенно возрастает риск утраты, изменения либо ненадлежащего закрепления электронных сведений, а также последующего вероятного признания их недопустимыми доказательствами по уголовному делу. Г. С. Русман, М. С. Смолин подчеркивают, что ст. 164.1 УПК РФ требует участия специалиста лишь в следственных действиях,

---

[196] Козловский П. В., Седельников П. В. Участие специалиста в изъятии электронных носителей // Научный вестник Омской академии МВД России. 2014. № 1. С.18.

[197] Приложение № 2 к диссертации (вопрос № 9).

[198] Приложение № 3 к диссертации (вопрос № 5).

связанных с изъятием электронных носителей информации, оставляя открытым вопрос о том, необходим ли такой специалист при копировании данных из электронных систем – носителей цифровой информации или получении информации из электронной системы на неэлектронном носителе – при изготовлении бумажных документов с использованием принтера[199]. В данной связи А. Р. Маламагамедова обоснованно отмечает, что все чаще в процессе доказывания должностные лица сталкиваются с цифровой информацией, электронными носителями информации, работой с сетью Интернет, которые требуют специальных знаний для обнаружения, собирания и оценки объектов и самой информации на предмет возможности их использования в качестве доказательств[200].

К обозначенным выше ситуациям относятся: 1) необходимость извлечения «летучих» электронных сведений (сохраняющихся только при включенном электронном устройстве и исчезающих при выключении или перезагрузке указанного устройства); 2) потребность в работе с защищенными электронными устройствами и электронными сведениями (наличие шифрования, пароля, биометрии, риска дистанционного удаления); 3) целесообразность создания криминалистически корректной электронной копии, требующей специальных технических средств и приемов для обеспечения неизменности полученных электронных сведений, включая закрепление параметров носителя и контрольных значений; 4) необходимость извлечения электронных сведений из распределенных и сетевых источников электронных данных (серверы, RAID-массивы, виртуальные среды, облачные сервисы), определения подлинности и целостности электронных файлов с использованием хэш-сумм, метаданных, электронных подписей; 5) потребность в восстановлении удаленной электронной информации с

---

[199] Русман Г. С., Смолин М. С. Правомочия стороны защиты в цифровом уголовном судопроизводстве // Правопорядок: история, теория, практика. 2026. № 1 (48). С. 169.

[200] Маламагамедова А. Р. «Электронные доказательства» в уголовном процессе // В сборнике: Уголовная политика России на современном этапе: состояние, тенденции, перспективы. Сборник научных трудов по материалам международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Г. А. Аванесова. В 2-х частях. М., 2024. С. 287-288.

поврежденных или модифицированных электронных носителей; 6) целесообразность проведения анализа сложных форматов электронных сведений, включающих видеозаписи, телекоммуникационные журналы, геолокационные сведения или электронные транзакции; 7) стремление установить наличие / отсутствие признаков вмешательства в содержание электронной информации, посредством повреждения электронного носителя, использования сокрытия или уничтожения цифровых следов, являющихся предметом исследования следователем и дознавателем в ходе расследования уголовного дела.

Дополнительным аргументом о необходимости привлечения специалиста к участию в отдельных процессуальных действиях выступают результаты эмпирического исследования. 31 % респондентов из числа должностных лиц органов предварительного расследования указали на возможность внесения изменений в содержание электронного доказательства, что влияет на признание его допустимым. Данный факт подтвердили 17 % адвокатов-защитников[201]. В указанных ситуациях участие специалиста выступает процессуальной гарантией сохранности электронных сведений, достоверности способа их получения, что обеспечивает надежную доказательственную базу по уголовному делу.

Верность утверждения о привлечении специалиста по усмотрению следователя и с учетом сложности процессуальной ситуации подтверждается и результатами анализа судебной практики, согласно которым суды, оценивая законность произведенных следователем, дознавателем процессуальных действий, опираются на действие принципа его процессуальной самостоятельности и признают право указанного субъекта по собственному усмотрению решать вопрос о необходимости привлечения специалиста для участия в обозначенных выше следственных действиях. Так, в судебных решениях неоднократно указывалось, что отсутствие специалиста при осмотре или изъятии электронных носителей само по себе не является безусловным основанием для признания доказательства

[201] Приложение № 2 к диссертации (вопрос № 10); Приложение № 3 к диссертации (вопрос № 6).

недопустимым, если иное не подтверждено материалами уголовного дела[202]. Первый кассационный суд общей юрисдикции, рассматривая жалобу защитника на незаконность действия субъекта расследования – получение флэш-носителя с видеозаписью в нарушение требований ст. 164.1 УПК РФ (отсутствие специалиста), не установил процессуальных нарушений при производстве следственного действия и указал на отсутствие данных, свидетельствующих о фальсификации и недопустимости собранных доказательств, оставив судебные решения нижестоящих судебных инстанций без изменения[203]. Тем самым подтверждается, что отсутствие специалиста при производстве рассматриваемых действий не влечет безусловного исключения электронного носителя из доказательственной базы в отсутствии конкретных нарушений закона, допущенных следователем, дознавателем, влияющих на принятие итогового решения по уголовному делу.

Подобная позиция судов усиливает право следователя, дознавателя самостоятельно определять степень технической сложности производства конкретного следственного действия, возможные риски, обусловленные таким производством, включая возможное ущемление прав подозреваемого, обвиняемого, и устанавливать необходимость привлечения специалиста к обозначенному производству. Можно констатировать, что судебная практика закрепляет правило, согласно которому участие специалиста расценивается не как обязательный элемент процессуальный формы следственного действия, а как дополнительное процессуальное средство установления фактических обстоятельств, применение которого зависит от усмотрения следователя,

---

[202] Кассационное определение Шестого кассационного суда общей юрисдикции от 27 ноября 2025 года № 77-3328/2025; Кассационное постановление Третьего кассационного суда общей юрисдикции от 18 сентября 2025 года по делу № 77-1758/2025; Кассационное постановление Девятого кассационного суда общей юрисдикции от 13 ноября 2025 года № 77-1609/2025; Кассационное постановление Шестого кассационного суда общей юрисдикции от 28 августа 2025 года № 77-2512/2025 // СПС «КонсультантПлюс» (дата обращения: 07.01.2026).

[203] Кассационное определение Первого кассационного суда общей юрисдикции от 17 декабря 2025 года по делу № 77-3884/2025 // СПС «КонсультантПлюс» (дата обращения: 08.01.2026).

дознавателя. Это, в свою очередь, создает предпосылки для формирования разнообразного правоприменения и снижения уровня защиты прав участников уголовного судопроизводства при использовании электронных доказательств в уголовно-процессуальном доказывании. Основа для этого создается и действующим правовым регулированием участия специалиста при изъятии электронных носителей информации и получении электронных сведений. Сохранение за следователем, дознавателем широкого усмотрения в решении вопроса о привлечении специалиста, подтверждаемое судебной практикой, с одной стороны, соответствует принципу процессуальной самостоятельности указанных субъектов, с другой же стороны, в условиях цифровизации процесса доказывания создает предпосылки для неоднозначного разрешения вопроса о допустимости, достоверности и достаточности электронных доказательств.

Негативные последствия указанного проявляются в нескольких взаимосвязанных аспектах. Во-первых, повышается риск процессуальных ошибок при обнаружении, изъятии, копировании, закреплении и хранении электронных сведений. Во-вторых, возрастает вероятность последующего признания электронных доказательств недопустимыми по причине нарушения порядка их получения, отсутствия подтверждения целостности и подлинности электронной информации, а также невозможности проверки неизменности ее содержания. В-третьих, отсутствие единых требований к использованию специальных знаний при собирании электронных доказательств влечет формирование неоднородной следственной практики, что не соответствует задачам уголовного судопроизводства и принципу правовой определенности.

С учетом изложенного следует признать, что участие специалиста при производстве следственных действий, связанных с изъятием электронных носителей информации и получением электронных сведений, должно рассматриваться не как дополнительное, необязательное процессуальное средство собирания электронных доказательств, а как важнейшая процессуальная гарантия в тех случаях, когда производство соответствующего действия сопряжено с повышенной технической сложностью получения электронных сведений, риском

изменения электронной информации либо вероятностью существенного ограничения прав личности. Вместе с тем обязательность участия специалиста не должна распространяться на все без исключения случаи обращения с электронными носителями, поскольку это способно неоправданно ограничить процессуальную самостоятельность следователя, дознавателя. Обоснованным является дифференцированный подход, при котором законодательно закрепляются случаи обязательного участия специалиста при производстве следственных действий.

В целях совершенствования правового регулирования уголовно-процессуального доказывания в части собирания электронных доказательств представляется необходимым в ст. 164.1 УПК РФ нормативно определить перечень обстоятельств, при которых участие специалиста обязательно; установить критерии отнесения следственной ситуации к числу технически сложных; предусмотреть процессуальную обязанность следователя, дознавателя мотивировать отказ от привлечения специалиста в случаях, связанных с обращением с электронным доказательством; определить порядок изъятия, копирования, закрепления и хранения цифровой информации, включая требования к обеспечению ее целостности и неизменности; конкретизировать случаи получения судебного решения при изъятии электронных сведений. Реализация указанных мер будет способствовать обеспечению разумного баланса между процессуальной самостоятельностью следователя, дознавателя и необходимостью использования специальных знаний в ходе уголовно-процессуального доказывания в условиях цифровой трансформации. Соответствующие предложения помещены в законопроект по совершенствованию УПК РФ[204].

Самостоятельным этапом, который часто является заключительным, собирания электронных доказательств выступает закрепление электронных сведений. Посредством такого закрепления электронные сведения приобретают юридическую силу. Учитывая, что электронная информация обладает рядом

[204] Приложение № 1 к диссертации.

свойств: большая подверженность изменению (в том числе вследствие автоматических процессов устройства и программ), допустимость получения множественности идентичных копий электронной информации, возможность утраты существенного контекста (метаданных, структуры хранения, сведений об учетной записи и условиях доступа), то доказательственное значение приобретает не только содержание электронных сведений, но и возможность достоверно подтвердить источник происхождения информации, ее принадлежность конкретному электронному объекту, отсутствие изменений в содержании между моментом получения и моментом исследования электронной информации.

В юридической литературе отмечается два подхода к пониманию закрепления электронных доказательств. Первый подход связан с процессуально-формальным (узким) пониманием[205] закрепления электронных доказательств. Он представляет собой фиксацию хода и результатов следственного (или иного процессуального) действия, в рамках которого обнаружены и получены электронные сведения, составление протокола процессуального действия и оформление приложений к нему (носителей с копиями, распечаток, фототаблиц, скриншотов и иных материалов). Данное понимание надлежаще отражает роль протокола процессуального действия как основной формы закрепления электронных сведений, однако недостаточно учитывает подтверждаемость неизменяемости электронных сведений.

Второй подход ассоциируется с процессуально-криминалистическим (расширенным) пониманием[206] закрепления электронных доказательств. Он включает в себя комплекс процессуальных и обеспечивающих мер, направленных на закрепление содержания электронных сведений и их реквизитов, идентификацию электронных сведений и их носителя, сохранение метаданных и контекста происхождения, исключение несанкционированного изменения и

---

[205] Кипнис Н. М. Допустимость доказательств в уголовном судопроизводстве. М.: Юрист, 1995. С. 63-67; Шейфер С. А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования: монография. М.: Норма, 2008. С.35-36.

[206] Россинская Е. Р. Теория судебной экспертизы (Судебная экспертология): учебник. М.: Норма : ИНФРА-М, 2026. С. 246.

создание условий для повторной проверки результата. Такое понимание закрепления электронных доказательств соответствует в большой степени сущности электронных доказательств, поскольку включает элементы, которые позволяют определить его достоверность.

Основывая на теории уголовно-процессуального доказывания (В. А. Лазарева, С. А. Шейфер и др.), учитывая изложенные мнения ученых, а также обозначенные выше особые свойства, признаки электронного доказательства, закрепление электронных доказательств по уголовным делам целесообразно определить как осуществляемую в рамках процессуального действия систему процессуального фиксирования и реализацию обеспечительных мер, направленных на закрепление содержания и идентифицирующих признаков электронных сведений и их носителей, отражение условий и способа получения электронной информации, обеспечение сохранности и неизменности полученных сведений, а также создание возможности их последующей проверки, исследования и оценки сторонами уголовного процесса и судом.

Протокол следственного действия является основной формой закрепления хода, условий, способов и результатов обнаружения, восприятия, изъятия и фиксации доказательственной информации, поскольку он отражает источник электронных сведений, действия следователя, дознавателя, результат извлечения информации. Согласно ст. ст. 166, 167 УПК РФ протокол следственного действия должен содержать сведения о времени, месте и обстоятельствах его проведения, действиях участников и обнаруженных объектах. Применительно к электронным сведениям в протоколе подлежит указанию информация об источнике получения электронных данных, характеристиках электронного носителя или файла, способе извлечения информации и действиях, совершенных субъектом расследования при работе с электронными сведениями. Распространенным недостатком в следственной практике выступает использование указанным властным субъектом общих формулировок без индивидуальных признаков электронного носителя и электронных объектов (например, указывается «файл с видеозаписью», атрибуты

его не приводятся)[207], что снижает проверяемость электронных свойств и дает основания для обжалования решений следователя, дознавателя.

Анализ уголовно-процессуальной практики свидетельствует о том, что субъекты расследования нередко допускают процессуальные нарушения при приобщении электронных доказательств к материалам уголовного дела. В частности, при составлении протоколов следственных действий в них надлежащим образом не указываются индивидуальные признаки полученных электронных файлов, носителей и упаковки изъятого, ввиду чего возникает риск замены электронных носителей информации и, соответственно, файлов, приложенных к протоколам следственных действий. Результаты эмпирического исследования позволили уточнить причину таких нарушений – отсутствие в УПК РФ процессуального порядка собирания электронных доказательств и их приобщения к материалам уголовного дела. На данный факт указали 38 % респондентов из числа следователей, дознавателей, 32 % адвокаты-защитники[208]. 23 % опрошенных субъектов расследования подчеркнули невозможность изъятия и приобщения к уголовному делу первоисточника электронных сведений. Аналогичную проблему отметили адвокаты-защитники[209].

Ненадлежащее закрепление электронных доказательств в уголовном судопроизводстве влечет существенные негативные последствия как для достижения целей доказывания, так и для обеспечения прав личности в уголовном процессе. Это проявляется, прежде всего, в снижении возможности проверить электронное доказательство. Если в протоколе следственного действия не отражены индивидуальные признаки электронного носителя, файла, учетной записи, особенности способа доступа, технических параметров копирования и

---

[207] Постановление Первого кассационного суда общей юрисдикции от 11 февраля 2025 года № 77-469/2025; Определение Первого кассационного суда общей юрисдикции от 31 января 2024 года № 77-454/2024, 77-6309/2023; Кассационное определение Четвертого кассационного суда общей юрисдикции от 01 марта 2022 года № 77-852/2022 // СПС «КонсультантПлюс» (дата обращения: 12.05.2026).

[208] Приложение № 2 к диссертации (вопрос № 10); Приложение № 3 к диссертации (вопрос № 6).

[209] Приложение № 2 к диссертации (вопрос № 10); Приложение № 3 к диссертации (вопрос № 6).

иных обстоятельств получения информации, то становится затруднительным установление того, что исследуемые в дальнейшем сведения тождественны тем, которые были фактически обнаружены и изъяты. Указанная неопределенность создает риск подмены электронного объекта, внесения в него изменений, утраты части данных либо искажения их содержания. Вследствие этого существенно усложняется последующая оценка доказательства судом, поскольку содержание электронных сведений без подтвержденного источника происхождения, без описания способа их извлечения и без сохранения метаданных не может рассматриваться как полностью проверяемое.

Не менее значимым негативным последствием неверного закрепления электронного доказательства выступает повышение вероятности признания электронного доказательства недопустимым. Электронные сведения, потенциально обладающие высоким доказательственным значением, могут быть исключены из доказательственной базы, что отрицательно сказывается на полноте, объективности расследования и эффективности судебного разбирательства по уголовным делам. Кроме того, отсутствие четкого нормативного порядка приобщения электронных доказательств к материалам уголовного дела способствует формированию неоднородной следственной и судебной практики, когда аналогичные по своему содержанию электронные сведения оформляются и оцениваются по-разному, что не соответствует требованиям правовой определенности и предписаниям ч. 2 ст. 1 УПК РФ.

Вышеизложенное актуализирует необходимость соблюдения субъектом расследования основных методических рекомендаций по работе с электронной информацией и ее носителями[210]. Под такими рекомендациями следует понимать совокупность выработанных в криминалистике и экспертной практике организационно-технических и процессуальных правил, обеспечивающих проверяемость происхождения электронных сведений, их неизменность и

[210] Галяшина Е. И., Шамаев Г. П. Обеспечение достоверности материалов оперативно-розыскных мероприятий как доказательств в уголовном судопроизводстве // Криминалистика и судебная экспертиза. СПб., 2012. С. 498.

воспроизводимость порядка получения последних. Разработчиками указанных рекомендаций выступают профильные ведомства (Следственный комитет России, МВД России, Минюст России), которые обобщают практику и разрабатывают правила по обнаружению, изъятию, копированию, упаковке и хранению электронных носителей и электронной информации. Полезным в данном случае является международный опыт по собиранию, получению и сохранению электронных доказательств, нормативно закрепленный в виде стандартов ISO/IEC 27037, 27041–27043 и др., устанавливающих принципы минимизации изменений, воспроизводимости порядка и полного закрепления действий с электронными сведениями. С учетом указанного диссертантом разработаны Методические рекомендации по закреплению электронных доказательств, помещенные в приложение к диссертации[211].

Всем этапам собирания электронных доказательств присущ риск необоснованного вмешательства в сферу частной жизни человека. Изъятие мобильных устройств, компьютеров, внешних накопителей, доступ к облачным хранилищам, переписке в мессенджерах, электронной почте и иным персонализированным электронным ресурсам затрагивают конституционное право на неприкосновенность частной жизни, личной и семейной тайны, закрепленное в ст. 23 Конституции РФ, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Наряду с этим предписания ст. 24 Конституции РФ запрещают сбор, хранение, использование и распространение информации о частной жизни лица без его согласия, если иное не предусмотрено законом. Данные конституционно-правовые положения корреспондируют требованиям ст. 7 УПК РФ – обязательность соблюдения законности в уголовном судопроизводстве, ст. 9 УПК РФ – об уважении чести и достоинства личности, ст. 11 УПК РФ – об охране прав и свобод человека и гражданина в уголовном судопроизводстве, а также нормам, регламентирующим производство следственных действий (ст. 164 УПК РФ) – об общих правилах их производства.

[211] Приложение № 5 к диссертации.

При отсутствии в уголовно-процессуальном законе четкого указания на допустимость собирания, копирования и исследования только тех сведений, которые относятся к предмету доказывания, возрастает риск чрезмерного вмешательства в личную сферу человека, а также необоснованного включения в уголовный процесс электронных сведений, не имеющих отношения к расследуемому событию. Кроме того, изъятие первоначальных носителей информации без надлежащего обоснования и без создания достоверной копии содержащихся на них данных, может повлечь ограничение имущественных, профессиональных и информационных интересов лица, лишая его возможности пользоваться необходимыми устройствами и содержащимися на них данными. Указанные действия способны ограничивать не только права, законные интересы подозреваемого, обвиняемого, но и потерпевшего, свидетеля, владельца устройства, а также иных лиц, сведения о которых оказались размещенными на соответствующем носителе. Ненадлежащее закрепление процессуальной формы электронных доказательств затрагивает сферу гарантированных законом прав личности. Прежде всего, это выражается в риске нарушения права обвиняемого на защиту, поскольку неполное или формальное закрепление электронных сведений существенно ограничивает возможность стороны защиты удостовериться в порядке происхождения информации.

Анализ материалов уголовных дел свидетельствует о том, что в ходе производства следственных действий, в частности осмотра места происшествия, обыска и выемки, следователь, дознаватель изымают различные электронные носители информации – мобильные телефоны, планшеты, ноутбуки и иные устройства[212]. В дальнейшем субъект расследования в рамках осмотра изъятых предметов получает возможность исследовать содержимое этих электронных носителей информации, включая сведения о датах, времени и продолжительности соединений, номерах абонентов, с которыми взаимодействовал владелец

[212] Материалы уголовного дела № 12202280013040012. СУ СК России по Тверской области; материалы уголовного дела № 12302520006000081. СУ СК России по Омской области; материалы уголовного дела № 12401460024000312. СУ УМВД России по Наро-Фоминскому городскому округу.

устройства, информацию о полученных сообщениях, а также содержание переписки.

Из содержания п. 11 Постановления Пленума Верховного Суда Российской Федерации от 01.06.2017 № 19 следует, что получение сведений о соединениях между абонентами, а также иных аналогичных данных допускается в рамках следственного действия, предусмотренного ст. 186.1 УПК РФ, и только на основании судебного решения[213]. Часть 7 ст. 185 УПК РФ предусматривает, что следователем по решению суда могут быть проведены осмотр и выемка электронных сообщений или иных передаваемых по сетям электросвязи сообщений, которые могут содержать сведения, имеющие значение для уголовного дела. Вместе с тем, правовая позиция о необязательности судебного разрешения на осмотр мобильного телефона получила отражение в практике Верховного Суда Российской Федерации[214]. В дальнейшем данный подход был подтвержден судами и одновременно разъяснено, что производство следственного действия в виде осмотра устройств, включая мобильные телефоны, не требует получения специального судебного решения[215].

В ряде определений Конституционный Суд Российской Федерации отметил, что осмотр и экспертное исследование данных, локально содержащихся в памяти правомерно изъятого электронного устройства, не требуют специального судебного решения[216]. Впоследствии Суд уточнил, что достаточность

---

[213] Постановление Пленума Верховного Суда Российской Федерации от 01 июня 2017 года № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

[214] Кассационное определение Верховного Суда Российской Федерации от 30 сентября 2014 года по делу № 2-18/08 // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

[215] Апелляционное определение Верховного Суда Российской Федерации от 1 августа 2019 года по делу № 2-003/2018 // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

[216] Определения Конституционного Суда Российской Федерации от 25 января 2018 года № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации», от 17 июля 2018 года № 1955-О «Об отказе в принятии к рассмотрению жалобы гражданина Сидака Константина Петровича на нарушение его конституционных прав частью шестой статьи 164 и статьей 177 Уголовно-процессуального

последующего судебного контроля в подобных случаях обусловлена осведомленностью лица об изъятии устройства и наличием у него возможности обратиться за судебной защитой, тогда как доступ к сведениям с использованием технических возможностей оператора связи предполагает необходимость предварительного судебного контроля[217].

В. С. Черкасов, не соглашаясь с вышеуказанными позициями Конституционного Суда Российской Федерации, считает необходимым распространить режим тайны связи на изъятый в ходе следственных действий электронный носитель информации[218]. По мнению И. А. Даниленко и Н. В. Васильева, тайна коммуникаций, независимо от формы ее выражения, должна обеспечиваться эффективными гарантиями от чрезмерного вмешательства со стороны государства, прежде всего посредством судебного контроля[219]. Схожей позиции придерживается и С. А. Грачев, также подчеркивающий необходимость усиленной процессуальной охраны соответствующей информации[220]. В свою очередь А. М. Багмет и С. Ю. Скобелин полагают, что исследование в ходе осмотра таких данных, как заметки, записи в календаре, фотографии, а также сведения о телефонных вызовах, не требует

кодекса Российской Федерации», от 28 ноября 2019 года № 3205-О «Об отказе в принятии к рассмотрению жалобы гражданина Габашвили Игоря Сергеевича на нарушение его конституционных прав частью первой статьи 176 и частью второй статьи 177 Уголовно-процессуального кодекса Российской Федерации»// СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

[217] Определение Конституционного Суда Российской Федерации от 24 июня 2021 года № 1364-О «Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

[218] Черкасов В. С. Почему в российском уголовном процессе необходимо совершенствовать гарантии защиты тайны «электронных коммуникаций»? // Вестник Московского университета МВД России. 2021. № 4. С. 130

[219] Даниленко И. А., Васильев Н. В. Соблюдение конституционных прав личности на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, почтовых, телеграфных и иных сообщений при осмотре мобильного устройства (российский и зарубежный опыт) // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 10. С. 154.

[220] Грачев С. А. Конституционные права личности при осмотре мобильного устройства: коллизия толкований в правовых позициях высших судебных инстанций России требует законодательного разрешения // Вестник Восточно-Сибирского института МВД России. 2020. № 3 (94). С. 142-143.

предварительного получения судебного разрешения[221], при этом ученые отмечают, что в ситуациях, когда сотовый телефон участника уголовного судопроизводства изъят и находится у следователя, получать судебное решение на его осмотр и ознакомление с цифровым содержимым не требуется[222]. А. Н. Яковлев считает, что «сообщения, передаваемые по электронной почте, перестают охраняться тайной связи в момент получения сообщения на устройстве пользователя, так как операторы связи передали информацию на устройство пользователя, тем самым сняли с себя ответственность по ее сохранности. По мнению автора, судебное решение необходимо только в тех случаях, когда информация находится в технической ответственности операторов связи. В иных случаях данные могут быть получены в порядке ст. 86 УПК РФ в ходе производства следственных действий без судебного санкционирования»[223].

Изъятие электронных носителей информации создает для следователя, дознавателя возможность доступа не только к данным, локально содержащимся в памяти устройства, но и, при наличии сохраненной авторизации, к сведениям, размещенным во внешних электронно-информационных сервисах, включая переписку в социальных сетях и мессенджерах, а также данные облачных хранилищ. При этом, исходя из правовых позиций Конституционного Суда Российской Федерации, специальное судебное разрешение на исследование содержимого правомерно изъятого устройства не требуется. Вследствие этого в правоприменительной практике возникает риск фактически неограниченного доступа к значительному объему электронных сведений личного характера без необходимого разграничения между локально хранящимися и удаленными данными, что ставит вопрос о необходимости дополнительного уточнения пределов ограничения конституционных прав личности. Отмеченное

[221] Багмет А. М., Скобелин С. Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. № 2. С. 22-27.

[222] Багмет А. М., Скобелин С. Ю. Пределы ограничения конституционных прав граждан в ходе осмотра сотовых телефонов участников уголовного судопроизводства // Уголовное право. 2017. № 6. С. 103.

[223] Яковлев А. Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «Электронная почта» // Вестник Воронежского института МВД России. 2014. № 4. С. 42-48.

подтверждается и правовыми позициями Конституционного Суда Российской Федерации и Верховного Суда Российской Федерации.

Допустимость доступа к электронной информации должна определяться с учетом специфики источника электронных сведений, способа их получения, степени вмешательства в сферу частной жизни и тайны сообщений, а также рисков их видоизменения или утраты. Это обусловливает необходимость разграничения процессуального режима получения локально содержащихся, удаленных и операторских данных и установления для них дифференцированных процессуальных гарантий в виде осуществления судебного контроля. На данную проблему в уголовно-процессуальной науке обращали внимание многие ученые, что свидетельствует о ее устойчивой научной и практической значимости[224].

Представляется, что ключевым требованием определения допустимых пределов ограничения конституционных прав личности при собирании электронных доказательств должна выступать специфика источника электронных сведений. В этой связи целесообразно разграничивать как минимум три группы электронных сведений: 1) локальные электронные данные, содержащиеся в памяти законно изъятого устройства; 2) удаленные электронные данные, доступ к которым осуществляется через законно изъятое устройство, но которые находятся вне его памяти; 3) электронные данные, находящиеся у оператора связи, провайдера либо иного внешнего субъекта.

---

[224] Юрченко И. А. Нарушение телекоммуникационной тайны в контексте российского уголовного права: текущие проблемы и перспективы их преодоления // Lex russica. 2023. Т. 76. № 9. С. 44; Даниленко И. А., Васильев Н. В. Соблюдение конституционных прав личности на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, почтовых, телеграфных и иных сообщений при осмотре мобильного устройства (российский и зарубежный опыт) // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 10. С. 150-157; Черкасов В. С. Тайна «Электронных коммуникаций» в уголовном процессе России, США, Китая и Германии // Проблемы правовой и технической защиты информации. 2020. № 8. С. 114-115; Грачев С. А. Тайна телефонных переговоров в правовых позициях высших судебных инстанций России: коллизия толкований // Законы России: опыт, анализ, практика. 2020. № 2. С. 81-85; Литвин И. И. Некоторые особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2020. № 1 (53). С. 9; Фильченко А. П., Жандров В. Ю. Соблюдение законности при получении информации с электронных мобильных устройств, принадлежащих задержанным // Российское правосудие. 2018. № 3 (143). С. 85-91.

Применительно к локально хранящимся данным допустимо согласиться с позицией Конституционного Суда Российской Федерации о том, что их исследование в рамках осмотра законно изъятого устройства не требует обязательного предварительного судебного решения. Однако и в этом случае вмешательство должно быть ограничено лишь теми электронными сведениями, которые связаны с предметом доказывания, поскольку сам факт изъятия электронного устройства не может оправдывать исследование всей содержащейся в нем информации.

Иной процессуальный порядок необходим в отношении удаленных и операторских электронных данных. Доступ к ним сопряжен с более интенсивным вмешательством в сферу частной жизни, тайны сообщений, поэтому требует усиления процессуальных гарантий – прежде всего получение предварительного судебного разрешения. При этом следует учитывать и технологические особенности электронной информации, выражающиеся в риске ее видоизменения или утраты. Указанное обстоятельство может обусловливать необходимость производства неотложных действий по осмотру и сохранению таких данных без предварительного судебного решения, однако с последующим незамедлительным уведомлением суда и проверкой законности, обоснованности и соразмерности произведенного вмешательства. Тем самым обеспечивается баланс между потребностью в оперативном собирании и сохранении электронных доказательств и необходимостью соблюдения конституционных гарантий прав личности. Вышеуказанные предложения целесообразно закрепить в УПК РФ[225].

Таким образом, пределы ограничения конституционных прав личности при собирании электронных доказательств должны определяться с учетом источника электронных сведений, способа доступа к ним и риска их утраты, что предполагает дифференциацию процессуальных режимов получения локальных, удаленных и операторских данных.

Представляется необходимым внесение изменений в ст. 166 УПК РФ, предусматривающих дополнение перечня обязательных реквизитов протокола

[225] Приложение № 1 к диссертации.

следственного действия специальными требованиями, применяемыми в случаях работы с электронными сведениями. В частности, в протоколе должны обязательно указываться индивидуальные признаки электронного объекта, последовательность действий по его обнаружению и извлечению, технические средства, примененные при копировании, сведения о лицах, осуществлявших соответствующие действия, результаты проверки целостности данных, способ упаковки электронного носителя, а также информация о приложениях к протоколу следственного действия в виде электронных носителей, распечаток, скриншотов, фототаблиц и иных материалов. Для обеспечения системности правового регулирования в рассматриваемой части ст. 166 УПК РФ необходимо дополнить предписаниями, конкретизирующими порядок оформления приложений к протоколу: порядок подписания, упаковки, маркировки и хранения электронных носителей и копий цифровой информации. Соответствующие предложения помещены в законопроект по совершенствованию УПК РФ[226].

На основании изложенного можно сформулировать следующие выводы.

1. Доказательственное значение электронные сведения способны приобрести при соблюдении субъектом расследования специальных правил по обнаружению и изъятию источника электронных данных, сохранению и закреплению последних, которые коррелируют с общими положениями теории уголовно-процессуального доказывания.

2. Обязательная фиксация содержания электронных сведений, их идентифицирующих признаков, способа получения таких сведений обеспечивает последующую проверку электронных доказательств, создавая тем самым условия для придания им юридической силы в уголовном судопроизводстве.

3. Совершенствованию процессуального порядка собирания электронных доказательств будет способствовать нормативное закрепление процессуальных правил, предусматривающих безотлагательное сохранение электронных сведений, имеющих значение для уголовного дела, случаи обязательного участия специалиста при их получении.

---

[226] Приложение № 1 к диссертации.

§ 2.2. Особенности проверки и оценки электронных доказательств в ходе предварительного расследования

Развитие цифровых технологий и расширение использования электронных сведений в уголовном процессе ставят вопрос о необходимости пересмотра традиционных взглядов не только на собирание, но и на проверку, оценку доказательств. Относительно проверки электронных доказательств А. А. Количенко отмечает, что современная следственная практика характеризуется устойчивым ростом случаев изъятия электронных носителей информации и копирования содержащихся на них сведений, что обусловливает необходимость совершенствования механизмов обозначенной проверки[227]. Полагаем, что процессуальная форма проверки электронных доказательств находится пока на этапе формирования. Это обусловлено как сущностью, особенными свойствами самих электронных сведений, так и недостаточной разработанностью процессуальных правил обращения с ними. Кроме того, в действующем уголовно-процессуальном законодательстве отсутствует нормативно закрепленное, исчерпывающее по содержанию понятие проверки доказательств, равно как и прямое указание на его цели. Это осложняет теоретическое осмысление данного института и практическую реализацию в уголовном судопроизводстве.

В научной процессуальной литературе отсутствует единообразие в понимании проверки доказательств. Так, часть авторов отождествляет проверку доказательств с их исследованием[228], другие же авторы ставят под сомнение

---

[227] Количенко А. А. Отдельные аспекты проверки электронных доказательств в уголовном процессе // Проблемы юридической науки в исследованиях адъюнктов и соискателей: Сб. научн. трудов. М., 2022. Вып. 28. С. 107-116.

[228] Маслов А. Г. Проверка доказательств – средство обеспечения законности в уголовном судопроизводстве.// Межвуз. сборник науч. статей. Саратов, 1989. С.40

рассмотрение ее в качестве самостоятельного этапа в структуре доказывания[229]. Ряд исследователей связывает содержание проверки уголовно-процессуальных доказательств с уяснением и анализом имеющихся доказательств, а также с получением иных доказательств для подтверждения либо опровержения достоверности уже собранных сведений[230]. Вместе с тем в отдельных работах проверку наделяют характеристиками, традиционно относимыми к оценке доказательств, что приводит к смешению указанных понятий и затрудняет их разграничение в теории и правоприменении[231]. Представляется возможным рассматривать проверку доказательств как самостоятельный и одновременно взаимосвязанный с оценкой элемент процесса уголовно-процессуального доказывания. Проверка доказательств создает предпосылки для последующей оценки сведений, имеющих отношение к уголовному делу, поскольку без установления источников получения доказательств, исследования содержания последних и сопоставления с иными данными по уголовному делу невозможно сформировать надежную доказательственную базу.

Нормативные положения, определяющие порядок проверки доказательств, закреплена в ст. 87 УПК РФ. Они предусматривают, что проверка осуществляется путем: 1) сопоставления доказательства с другими доказательствами; 2) установления источников доказательства; 3) получения иных доказательств, подтверждающих либо опровергающих проверяемое доказательство. Данные положения распространяются на все виды уголовно-процессуальных доказательств. Однако в отношении к электронным доказательствам их

---

[229] Курс советского уголовного процесса. Общая часть. Под ред. А. Д. Бойкова и И. И. Карпеца. М. : Юрид. лит., 1989. С. 613-614; Ларин А. М. Расследование по уголовному делу: процессуальные функции. М. : Юрид. лит., 1986. С.19.

[230] Строгович М. С. Курс советского уголовного процесса. М. Изд-во Акад. наук СССР, 1968. Т.1. С. 303; Валяев А. И. Проверка доказательств как самостоятельный элемент процессуального доказывания // В сборнике Актуальные проблемы судоустройства, судопроизводства и прокурорского надзора. М., 1985. С. 108.

[231] Теория доказательств в советском уголовном процессе. М. : Юрид. лит., 1973. С. 333; Кокорев Л. Д., Кузнецов Н. П. Уголовный процесс: доказательства и доказывание. Воронеж : Изд-во Воронеж. ун-та. 1995. С. 220; Бирмамитова С. А. Доказывание на досудебных стадиях уголовного процесса по делам о преступлениях, совершенных осужденными в исправительных колониях: дис. ... канд. юрид. наук., М., 2007. С. 116.

применение приобретает особенности, обусловленные сущностью электронных сведений. Следует учитывать, что предусмотренные ст. 87 УПК РФ способы проверки доказательств реализуются в уголовном процессе посредством производства конкретных процессуальных действий и принятия процессуальных решений. Применительно к электронным доказательствам такими действиями выступают прежде всего: осмотр предметов и документов (ст. ст. 176, 177 УПК РФ), осмотр электронных носителей информации и содержащихся на них сведений, выемка и обыск электронных устройств (ст. ст. 182, 183 УПК РФ), истребование информации у организаций и операторов связи (ст. 86 УПК РФ), получение сведений о соединениях между абонентами (ст. ст. 186.1 УПК РФ), назначение судебной экспертизы (ст. 195 УПК РФ), привлечение специалиста (ст. ст. 58, 168 УПК РФ). Указанные процессуальные способы образуют процессуальный механизм проверки электронных доказательств, обеспечивающий их относимость, достоверность, допустимость в уголовном судопроизводстве

По справедливому замечанию А. В. Рудина, закрепленные в ст. 87 УПК РФ способы проверки доказательств отражают как мыслительную, так и практическую стороны осуществления данной деятельности[232]. Проверка электронных доказательств представляет собой сложную и многоаспектную процессуальную деятельность, что обусловлено особенностями создания, хранения и изменения электронной информации[233]. Мыслительная деятельность проявляется в анализе содержания электронных сведений, выдвижении гипотез о происхождении и механизме формирования электронных сведений, сопоставлении с иными доказательствами и проверке следственных версий. Практическая деятельность включает процессуальные действия по изъятию носителей электронных сведений, осмотру последних, получению сведений у операторов связи и сервисов, назначению судебных экспертиз, привлечению специалистов и т. д.

---

[232] Рудин А. В. Проверка доказательств в ходе досудебного производства в российском уголовном процессе: дис. … канд. юрид. наук. Краснодар, 2019. С. 67.

[233] Количенко А. А. О специфике проверки электронных доказательств в уголовном процессе // Альманах молодых ученых. 2022. № 2. С. 108-114.

В досудебном производстве проверка технических характеристик электронных доказательств выступает не формальностью, а ключевым средством недопущения ничтожности рассматриваемых доказательств, исключения принятия незаконных и необоснованных решений о предъявлении обвинения, избрании меры пресечения, форме окончании предварительного расследования.

Анализ уголовно-процессуальной практики, мнений респондентов по вопросу проверки электронных доказательств в ходе предварительного расследования свидетельствует о существовании ряда проблем, препятствующих эффективному установлению соответствия собранных по уголовному делу доказательств предъявляемым уголовно-процессуальным законом требованиям. В развитие указанного отметим, что одним из ключевых способов проверки электронных доказательств в следственной практике является их сопоставление с иными доказательствами по уголовному делу. Как отмечается в научной литературе, с помощью определенного алгоритма можно выявить взаимосвязи и закономерности между доказательствами, что ускоряет процесс расследования[234].

Одной из распространенных проблем проверки электронных доказательств является использование производных форм закрепления электронной информации (скриншотов, фототаблиц, распечаток) вместо первоначального источника электронных сведений[235]. В следственной практике встречаются нередкие случаи, когда при изъятии следователем телефона в протоколе следственного действия отсутствует описание действий по доступу к устройству, однако к материалам уголовного дела приобщаются фототаблицы переписки. Это вызывает сомнения в

---

[234] Рябинина Т. К., Чистилина Д. О. Перспективные направления использования искусственного интеллекта в доказывании по уголовным делам // Проблемы правоохранительной деятельности. 2025. № 3. С. 23.

[235] Приговор Останкинского районного суда города Москвы от 24 марта 2026 года по делу № 1-250/2026; Приговор Кузьминского районного суда города Москвы от 29 января 2026 года по делу № 1-0108/2026; Приговор Никулинского районного суда города Москвы от 29 мая 2025 года по делу № 1-0223/2025// Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

происхождении электронных сведений и требует последующего проведения судебной экспертизы[236].

Вышеуказанное не коррелирует с общими требованиями уголовно-процессуального закона, предъявляемыми к доказательствам и доказыванию (ст. ст. 74 и 85 УПК РФ). Значение имеет не только содержание полученных сведений, но и процессуальная форма их закрепления, что обеспечивает возможность проверки их происхождения, целостности, неизменности, достоверности. Научная и практическая значимость обозначенной проблемы обусловлена тем, что производные формы закрепления электронной информации, в отличие от первоначальных цифровых данных, как правило, не содержат метаданные[237] и иные технические характеристики (временные параметры создания, изменения и сохранения данных, сведения о типе устройства, операционной системе и используемом программном обеспечении, данные о формате, структуре и свойствах файла, сетевые параметры, сведения о цифровом пути формирования и передачи информации, а также данные системных журналов), позволяющие установить источник происхождения сведений, условия их формирования, последовательность доступа к ним, признаки изменения. Вследствие указанного существенно затрудняется установление происхождения электронной информации, невозможным становится достоверно определить, с какого устройства, из какого приложения, аккаунта либо иного цифрового источника были получены сведения, кем, когда и в какой последовательности осуществлялся доступ к ним, а также соответствует ли представленный в уголовном деле материал тому содержанию, которое объективно существовало на момент производства следственного действия. Если в протоколе следственного действия не отражены способ доступа к устройству, параметры программной

---

[236] Материалы уголовного дела № 12401460024000312. СУ УМВД России по Наро-Фоминскому городскому округу; материалы уголовного дела № 12501280014000105. Нелидовский МСО СУ СК России по Тверской области.

[237] Метаданные – это совокупность структурированных атрибутов электронных сведений, отражающих технические, временные, идентификационные и иные характеристики цифрового объекта, необходимые для его описания, систематизации, поиска, обработки, интерпретации и подтверждения подлинности.

среды, системное время[238], последовательность действий должностного лица при обращении с электронными данными и характеристики исследуемого цифрового ресурса, то процесс формирования доказательственной информации остается неустановленным. Между тем общие требования к составлению протокола следственного действия закреплены в ст. ст. 166, 167 УПК РФ, применительно к протоколу осмотра – также в ст. ст. 176, 177 УПК РФ. Ненадлежащее отражение в протоколе следственного действия порядка получения цифровых сведений исключает возможность проверки полноты законности их получения.

Существенным негативным последствием отмеченной ситуации является и ограничение возможности проверки целостности и неизменности электронной информации. Исходные электронные данные содержат метаданные, временные отметки, сведения о формате, параметрах создания и изменения объекта, имеющие значение для установления неизменности доказательственного материала. На данный факт обращает внимание Г. С. Русман[239]. Использование производных форм фиксации электронных сведений лишает следователя, дознавателя возможности исследовать эти характеристики в полном объеме. В результате затрудняется выявление признаков редактирования, выборочного копирования, удаления фрагментов, монтажа и иного воздействия на содержание электронных сведений. Это объективно снижает степень доказательственной надежности электронных сведений, что должно учитываться при ее оценке по правилам ст. 88 УПК РФ.

Отдельного внимание заслуживает утрата содержательного[240] и технического контекста электронной информации[241] в ходе ее извлечения,

---

[238] Системное время – это внутренне установленный в компьютере, мобильном устройстве, сервере либо иной информационной системе временной параметр, на основе которого осуществляется регистрация моментов создания, изменения, сохранения, передачи, доступа и иных действий с электронными данными.

[239] Русман Г. С., Смолин М. С. Правомочия стороны защиты в цифровом уголовном судопроизводстве // Правопорядок: история, теория, практика. 2026. № 1 (48). С. 170.

[240] Содержательный контекст электронной информации – это сведения о смысловом содержании данных, их связи с иными сообщениями, документами, событиями и действиями пользователей, необходимые для правильного понимания значения такой информации.

[241] Технический контекст электронной информации – это сведения о технических условиях создания, обработки, передачи, отображения и хранения электронной информации,

копирования, преобразования формата, переноса на иные носители, распечатки, а также последующего процессуального оформления и приобщения к материалам уголовного дела. Производное визуальное отображение цифровой информации, зафиксированное на определенном устройстве конкретным лицом**,** фиксирует лишь ограниченный фрагмент цифровой среды и не позволяет исследовать весь комплекс сопутствующих данных, способных иметь значение для установления обстоятельств, подлежащих доказыванию в соответствии со ст. 73 УПК РФ. За пределами такой фиксации нередко остаются сведения о полном массиве коммуникации между участниками уголовного судопроизводства, статусе сообщений, представляющих интерес для уголовного дела, последовательности их отправки и получения, данных профиля пользователя – подозреваемого, обвиняемого, потерпевшего, свидетеля, вложениях, системных отметках и иных элементах цифровой инфраструктуры. Вследствие этого предметом проверки становится не целостный цифровой объект, а его фрагментарное отображение, что создает риск искажения фактической картины, представляющей интерес для установления обстоятельств совершенного преступления.

Рассматриваемая практика затрагивает и гарантированные законом права личности. Прежде всего речь идет о праве на защиту, закрепленном в ст. 48 Конституции Российской Федерации и ст. 16 УПК РФ, приобщении к уголовному делу лишь производных форм электронной информации, что ограничивает возможности стороны защиты по их полноценному исследованию, поскольку отсутствие доступа к первоначальному электронному источнику исключает постановку содержательных вопросов о происхождении электронных сведений, их содержании, полноте и признаках возможной модификации. Г. С. Русман, М. С. Смолин по данному поводу отмечали, что проблема собирания, представления, оценки цифровых следов, а также использования

включая данные об устройстве, программной среде, времени, формате, метаданных, сетевых параметрах и иных характеристиках, способных повлиять на восприятие, интерпретацию и оценку такой информации.

возможностей электронного документооборота стороной защиты содержит в себе «логическое» и «процессуальное» измерения[242].

Придание доказательственного значения сведениям, происхождение и неизменность которых не подтверждены вследствие использования следователем дознавателем производных форм закрепления электронной информации, способно повлечь невозможность надлежащей защиты права потерпевшего, гарантированного ст. 52 Конституции Российской Федерации, при наличии фактически существующих, но ненадлежащим образом закрепленных электронных следов преступления. В этом контексте следует учитывать и положение ч. 3 ст. 49 Конституции Российской Федерации, согласно которому неустранимые сомнения в виновности лица толкуются в пользу обвиняемого.

Необходимость преодоления указанных сложностей проверки уголовно-процессуальных доказательств в условиях цифровизации дополнительно подтверждают верность предлагаемого в параграфе 1 главы 2 настоящего исследования дополнения ст. 74 УПК РФ предписаниями об использовании сведений в электронной форме в доказывании прежде всего в их первоначальном электронном виде либо в форме криминалистически корректной копии.

Самостоятельной проблемой проверки, сопряженной с осуществлением надлежащей оценки, электронных доказательств на стадии предварительного расследования выступает неверное установление и интерпретация следователем, дознавателем временных характеристик электронных сведений[243], а равно иных метаданных, отождествляющих цифровые объекты. Существование указанной проблемы обусловлена тем, что электронные доказательства, в отличие от вещественных доказательств и документальных источников информации, имеют доказательственную ценность не только ввиду их информационного содержания, но и совокупности их технических параметров, позволяющих судить о времени создания, изменения, сохранения, передачи, копирования либо перемещения

[242] Русман Г. С., Смолин М. С. Правомочия стороны защиты в цифровом уголовном судопроизводстве // Правопорядок: история, теория, практика. 2026. № 1 (48). С. 167.

[243] Временные характеристики электронных сведений – это данные о времени и последовательности совершения операций с электронной информацией.

соответствующего объекта в цифровой среде. Вместе с тем такие параметры не могут презюмироваться как изначально достоверные, поскольку их содержание зависит от многих факторов технического и пользовательского характера, включая особенности настройки часового пояса, корректность отображения системного времени устройства, наличие / отсутствие автоматической синхронизации с серверами точного времени, использование облачных сервисов, перенос файла между различными устройствами, приложениями и каналами связи. Одним из подтверждений указанного является пример из следственной практики о расследовании незаконного оборота наркотических средств. В ходе производства по уголовному делу фотография с координатами предполагаемого тайника, обнаруженная в мобильном устройстве подозреваемого, была положена в основу вывода следователя о причастности лица к покушению на сбыт наркотических средств. Сторона защиты же ссылалась на несоответствие времени, содержащегося в свойствах изображения, моменту фактического задержания, а также на существующее противоречие между визуально воспринимаемой обстановкой, зафиксированной на фотографии, и реальными сезонными характеристиками периода изъятия наркотического средства. При этом на первоначальном этапе расследования не были установлены достоверность системного времени устройства, способ формирования либо появления файла в памяти телефона, возможный факт его получения посредством пересылки или загрузки, а также соответствие содержания изображения данным, отраженным в протоколе осмотра места происшествия[244]. В соответствии со ст. ст. 164, 176, 177, 180 УПК РФ следственные действия, производимые в целях обнаружения, осмотра и фиксации объектов, должны осуществляться с соблюдением требований законности и с надлежащим отражением существенных обстоятельств в протоколе соответствующего следственного действия. В подобных условиях использование такого цифрового объекта в качестве уголовно-процессуального

[244] Материалы уголовного дела № 12401460024000312. СУ УМВД России по Наро-Фоминскому городскому округу; материалы уголовного дела № 1250145045000025. СО ОМВД России по району Измайлово г. Москвы.

доказательства без дополнительной технической верификации его метаданных и сопоставления его содержания с иными материалами дела не отвечает критериям надлежащей проверки доказательств, вытекающим из ст. ст. 87, 88 УПК РФ. При отсутствии надлежащей верификации метаданных субъект расследования фактически подменяет исследование реальных параметров происхождения электронного объекта формальным восприятием его внешних характеристик, что обуславливает ошибочность его вывода о времени совершения деяния, последовательности действий участников уголовного судопроизводства, месте нахождения обвиняемого, наличии связи конкретного цифрового объекта с обстоятельствами, подлежащими доказыванию по уголовному делу. На данную проблему обращали внимание и Г. С. Русман, М. С. Смолин[245].

Негативные последствия обозначенной проблемы проявляются в следующем. Во-первых, не подтверждается достоверность электронного доказательства. Без установления условий формирования метаданных невозможно с необходимой степенью определенности утверждать, что содержащиеся в них временные параметры отражают действительный момент возникновения либо использования соответствующих электронных сведений. Во-вторых, относимость такого доказательства, так как отсутствие достоверных знаний о происхождении электронных сведений, способе их появления на устройстве и истории перемещения в цифровом пространстве не позволяют без сомнения соотнести его с расследуемым событием. В-третьих, недостатки проверки электронного доказательства неизбежно отражаются на процессе его оценки. В совокупности с иными материалами уголовного дела формируется риск построения ошибочной следственной версии, формирования доказательственной базы, в рамках которых предположительный по своей технической сущности электронный след приобретает значение подтвержденного обстоятельства.

Следствием указанных недостатков выступает не только снижение доказательственной ценности электронных сведений, но и создание предпосылок

[245] Русман Г. С., Смолин М. С. Правомочия стороны защиты в цифровом уголовном судопроизводстве // Правопорядок: история, теория, практика. 2026. № 1 (48). С. 170.

для признания их недостоверными, а при наличии процессуальных нарушений, связанных с порядком обнаружения, фиксации, изъятия и исследования, также и недопустимыми в соответствии со ст. 75 УПК РФ. В результате не только не достигается публичный интерес – правильное разрешение уголовного дела в разумный срок, но и нарушаются гарантированные права и законные интересы участников уголовного процесса.

С учетом изложенного в целях исключения неверного (необъективного) восприятия следователем, дознавателем временных характеристик и иных метаданных электронного объекта необходимо дополнить ст. 87 УПК РФ положением о том, что проверка электронных сведений осуществляется путем установления их происхождения, технических условий создания, изменения, хранения, передачи, обязательного сопоставления содержащихся в них метаданных с иными доказательствами по уголовному делу. Соответствующая специфика проверки электронных доказательств должна найти отражение и в ст. 88 УПК РФ, закрепляющей правила оценки доказательств, посредством прямого указания на недопустимость признания временных меток, геолокационных данных и иных метаданных достоверными без проверки условий их формирования и соотнесения с иными, собранными по уголовному делу доказательствами. Соответствующие предложения помещены в законопроект по совершенствованию УПК РФ[246].

Формирование надлежащей доказательственной базы по уголовному делу с использованием электронных доказательств осложняется также получением следователем, дознавателем беспрепятственного доступа к облачным сведениям, разграничением локальной памяти и серверного хранения в целях уголовно-процессуального доказывания. В тех случаях, когда в ходе осмотра телефона, планшета или иного цифрового устройства следователь, дознаватель подключает последний к сети Интернет, осуществляет вход в учетную запись, инициирует синхронизацию либо иным образом получает доступ к удаленным электронным сведениям, то возникает ситуация смешения различных по своей правовой и

[246] Приложение № 1 к диссертации.

технической природе источников информации. В результате этого становится затруднительным установление того, какие именно сведения находились в памяти устройства на момент его изъятия, а какие были получены дополнительно с сервера, из облачного хранилища, резервной копии или синхронизированного аккаунта. Подобная неопределенность негативно влияет на возможность последующей проверки доказательства, поскольку препятствует достоверному установлению источника происхождения информации, механизма ее появления на устройстве и условий, при которых она стала доступной субъекту расследования. Отмеченное не согласуется с предписаниями ст. ст. 73, 74, 85, 87 и 88 УПК РФ. При отсутствии точной фиксации сетевого режима устройства, факта подключения к Wi-Fi или мобильной сети, использования учетных данных, ввода паролей, проведения синхронизации и иных действий, связанных с обращением к облачной среде, существенно осложняется проверка того, в каком именно объеме и из какого источника были получены электронные сведения. Это, в свою очередь, создает сомнения в их достоверности, поскольку отображенные на экране сообщения, файлы, фотографии или иные данные могли отсутствовать в локальной памяти устройства и появиться только в результате сетевого взаимодействия с удаленным сервером. Вследствие этого становится проблематичным установить, существовали ли указанные сведения в том же виде на момент изъятия устройства, не подвергались ли они изменениям, восстановлению, обновлению либо повторной загрузке после начала следственного действия.

В. С. Удовиченко и С. А. Сорокина отмечают, что остается открытым вопрос о том, к какому виду доказательств относится информация, хранящаяся не в памяти электронного носителя, а в облачном хранилище. Они указывают на то, что доступ к такой информации возможен только при подключении к интернету, а это выходит за пределы изъятого объекта (телефона, ноутбука и т. д.). В связи с этим изъятие устройства у лица необязательно, так как доступ в интернет можно

осуществить с любого другого устройства[247]. И. П. Можаева и Е. П. Шульгина подчеркивают, что перед правоохранительными органами встает вопрос не только обнаружения, доступа, изъятия информации, имеющей доказательственное значение, но и правильного процессуального оформления этих действий[248].

Исследование материалов уголовного дела показало, что при осмотре телефона следователь подключил устройство к Wi-Fi, после чего в приложении появились ранее удаленные сообщения, восстановленные синхронизацией. Эти электронные сведения были отражены в протоколе осмотра как обнаруженные в памяти телефона. В дальнейшем обоснованно возникло сомнение у защитника о допустимости и правильности закрепления электронных сведений, поскольку не было ясно, были ли электронные сведения локальными или получены с сервера, а также какие действия по доступу к аккаунту осуществлялись[249]. Такое сомнение рождает основание ходатайствовать об исключении доказательства из доказательственной базы.

Отсутствие в уголовно-процессуальном законе правила о разграничения между локальными и облачными электронными данными оказывает существенное влияние на оценку доказательств с точки зрения их допустимости. Если сведения, фактически полученные из удаленного источника, фиксируются в протоколе как обнаруженные непосредственно в памяти устройства, то возникает нарушение процессуальной формы следственного действия. Осмотр предмета в таком случае фактически трансформируется в доступ к удаленной цифровой информации. Однако данное обстоятельство нередко не получает отражения в протоколе следственного действия, несмотря на требования закона о надлежащем порядке производства и фиксации хода следственных действий, закрепленные в ст. ст. 164, 166, 167, 176, 177 УПК РФ. Между тем обращение к облачным

[247] Удовиченко В. С., Сорокина С. А. Особенности изъятия информации с электронных носителей в досудебном производстве // Алтайский юридический вестник. 2021. № 2 (34). С. 133-138.

[248] Можаева И. П., Шульгин Е. П. О понимании доказательств в правоохранительной деятельности в эпоху цифровых преобразований // Юристъ-Правоведъ. 2022. № 4 (103). С. 162-167.

[249] Материалы уголовного дела № 11901460030000704. СО по г. Подольск ГСУ СК России по Московской области.

сведениям не сводится к обычному визуальному исследованию изъятого объекта, поскольку предполагает получение электронных данных, находящихся вне пределов материального носителя и потенциально существующих независимо от него. Это ставит под сомнение в ходе проверки электронного доказательства законность способа получения соответствующей информации, а также корректность ее закрепления в материалах уголовного дела. Более того, при отсутствии четкой фиксации в протоколе следственного действия технического механизма доступа к электронным сведениям затрудняется установление их связи с конкретным лицом, поскольку сам факт отображения информации на устройстве еще не означает, что она хранилась в его локальной памяти либо что именно владелец устройства в действительности ею распоряжался. Аналогичное мнение высказывает и П. А. Пастухов[250], Г. Н. Русман[251]. В условиях использования нескольких учетных записей, автоматической синхронизации, совместного доступа к сервисам или сохраненных сеансов авторизации решение следователем, дознавателем вопроса о принадлежности аккаунта, источника данных и фактического контроля над ними приобретает особую сложность. Следовательно, не разграничение указанных видов информации ослабляет доказательственную ценность электронных сведений, затрудняет их включение в систему доказательств и создает риск признания их недопустимыми на основании ст. 75 УПК РФ как полученных с нарушением требований уголовно-процессуального закона.

Наряду с трудностями процессуального характера проблема надлежащей проверки электронных доказательств затрагивает и сферу конституционно значимых прав личности. Подключение изъятого устройства к сети Интернет и последующее обращение к облачным сервисам способно существенно расширить пределы вмешательства в частную жизнь лица по сравнению с тем объемом

---

[250] Пастухов П. С. О необходимости замены в уголовном судопроизводстве письменного протокола электронным документом // Научный вестник Омской академии МВД России. 2015. № 3. С. 21.

[251] Русман Г. С., Смолин М. С. Правомочия стороны защиты в цифровом уголовном судопроизводстве // Правопорядок: история, теория, практика. 2026. № 1 (48). С. 168.

информации, который содержался непосредственно в памяти устройства на момент его изъятия. В результате субъект расследования потенциально получает доступ не только к локально сохраненным данным, но и к архивам переписки, резервным копиям, фотографиям, документам, геолокационным сведениям, контактам и иным массивам цифровой информации, размещенным в удаленной среде. Это повышает риск нарушения права на неприкосновенность частной жизни, личную и семейную тайну, гарантированного ст. 23 Конституции Российской Федерации.

С учетом изложенного представляется необходимым разграничивать локальные данные, содержащиеся в памяти устройства, и сведения, получаемые из облачной инфраструктуры в целях верного установления источника доказательственной информации, и повышение возможности ее проверки и оценки. Для этого целесообразно ст. 177 УПК РФ дополнить предписаниями об особенностях осмотра электронных устройств, в том числе о необходимости разграничения локально содержащихся данных от сведений, полученных посредством удаленного доступа или синхронизации. Наряду с этим представляется необходимым внесение уточнения в ст. 164 УПК РФ, установив общее правило о производстве осмотра цифровых устройств в условиях, исключающих изменение электронной информации вследствие автоматического сетевого взаимодействия, если иное не требуется в целях расследования уголовного дела и специально не отражено в протоколе следственного действия. Соответствующие предложения отражены в законопроекте по совершенствованию УПК РФ[252].

Проверка электронных доказательств предшествует этапу их оценки. В научной литературе понятие «оценка доказательств» раскрывается неоднозначно. Одни авторы понимают ее как логический процесс выявления связей между доказательствами, определения значения каждого доказательства и их совокупности для установления истины и принятия процессуального

[252] Приложение № 1 к диссертации.

решения[253]. Другие авторы рассматривают оценку как мыслительную, познавательную деятельность, направленную на установление свойств доказательств, закрепленных в ч. 1 ст. 88 УПК РФ[254]. Встречается мнение, согласно которому оценка выступает логическим продолжением проверки доказательств[255].

Наряду с отмеченным в доктрине уголовно-процессуального доказывания представлена позиция, согласно которой оценка уголовно-процессуальных доказательств рассматривается как мыслительная и практическая деятельность по формированию промежуточных и итоговых выводов об относимости, допустимости, достоверности и достаточности доказательств, необходимая для установления фактических обстоятельств дела, обоснования выводов и вынесения законного и обоснованного решения[256]. Ряд авторов акцентирует внимание на то, что оценка доказательств выражается в оценочных суждениях, а ее результатом является умозаключение о наличии либо отсутствии доказательства и о доказанности или недоказанности конкретного обстоятельства[257]. М. С. Строгович формулировку рассматриваемого понятия связывал с выводом о «доброкачественности» доказательства и о достоверной доказанности установленного им факта[258].

В развитие указанного подчеркнем, что по мнению В. А. Лазаревой, «оценка доказательств представляет собой мыслительную деятельность, включающую анализ и синтез содержания и процессуальной формы доказательства и завершающуюся выводом об относимости, допустимости и достоверности

---

[253] Белкин А. Р. Теория доказывания в уголовном судопроизводстве. М., 2007. С. 253.

[254] Крупницкая В. И. Теория доказательств и доказывание: курс лекций. Новосибирск. 2015. С.133.

[255] Кузнецов Н. П. Доказывание и его особенности на стадиях уголовного процесса России: дис. … докт. юрид. наук. Воронеж, 1998.С. 60.

[256] Балакшин В. С. Доказательства в теории и практике уголовно-процессуального доказывания (важнейшие проблемы в свете УПК Российской Федерации): дис. … д-ра юрид. наук. Екатеринбург. 2005. С. 152.

[257] Карпенко В. М. Оценка доказательств следователем и дознавателем: дис. … канд. юрид. наук. М., 2007. С. 35.

[258] Строгович М. С. Материальная истина и судебные доказательства в советском уголовном процессе. М, 1955. С. 289.

каждого доказательства, а также о достаточности их совокупности для принятия процессуального решения»[259]. И. Л. Петрухин отмечал, что «оценка доказательств реализует мыслительную деятельность следователей, дознавателей, прокуроров, судьи, которая осуществляется в логической форме при условии соблюдения научных методологий познаний, которая обеспечивается достижением истин»[260]. Л. М. Карнеева также придерживалась мнения о том, что «оценка доказательств – это всегда мыслительная деятельность, логическая операция, выражающаяся в оценочных суждениях»[261].

Обобщение доктринальных позиций ученых по вопросу оценки уголовно-процессуальных доказательств позволяет заключить, что при многообразии терминологии оценка доказательств в уголовном судопроизводстве преимущественно рассматривается как мыслительная (логико-познавательная) деятельность субъектов доказывания, направленная на формирование выводов об относимости, достоверности, допустимости каждого доказательства и достаточности их совокупности для принятия процессуального решения[262]. Мнения, включающие в понятие оценки доказательств компонент практической направленности, по существу сближают ее с проверкой доказательств, что свидетельствует о необходимости их четкого разграничения: практические действия властного субъекта уголовного судопроизводства относятся к осуществлению проверки доказательства, а оценка уголовно-процессуальных доказательств выражается в мотивированных умозаключениях и находит отражение в процессуальных решениях.

Процесс оценки уголовно-процессуальных доказательств следователем, дознавателем представляет собой мыслительную деятельность указанного

---

[259] Лазарева В. А. Доказывание в уголовном процессе: учебно-практическое пособие. М., 2009. С. 65.

[260] Петрухин И. Л. Теоретические основы реформы уголовного процесса в России. Часть II. М., 2015. С.67

[261] Карнеева Л. М. Судебная этика и тактика допроса // Этика предварительного следствия: Труды Высшей следственной школы МВД СССР. Волгоград, 1976. С. 49-62

[262] Ремизова М. С. Теоретические и правовые основы формирования допустимых доказательств в условиях состязательного уголовного процесса : дис. … канд. юрид. наук. Саратов, 2025. С. 146.

субъекта, результатом которой является формирование им выводов, закрепляемых в процессуальных решениях по уголовному делу. Поэтому следует согласиться с позицией Т. З. Егоровой о том, что «если бы оценка свелась исключительно к акту мысли, к только умственной операции, то она не вышла бы за границы сознания соответственного субъекта по уголовно-процессуальному доказыванию, была бы никому, помимо данного лица, не известная и лишалась бы любого своего значения правового характера»[263]. Таким образом, для понимания правовой составляющей этой мыслительной деятельности, следует обратиться к нормам уголовно-процессуального законодательства.

Согласно УПК РФ оценка уголовно-процессуальных доказательства предполагает: 1) установления соответствия каждого доказательства требованию относимости, допустимости, достоверности; 2) определение достаточности совокупности доказательств по уголовному делу для принятия процессуального решения на соответствующем этапе предварительного расследования. При этом действующее уголовно-процессуальное законодательство не содержит специальных норм, регулирующих особенности оценки электронных доказательств. Предписания ст. 88 УПК РФ устанавливают единые критерии оценки доказательств (относимость, допустимость, достоверность и достаточность), однако сущность, отличные свойства электронных доказательств в уголовно-процессуальном законе не учтены. Вследствие этого оценка электронных доказательств фактически осуществляется субъектом расследования по общим правилам, разработанным для традиционных доказательств, что не всегда позволяет объективно, полно учитывать специфику электронных сведений, создает риск ошибок в следственной практике.

В частности, анализ следственной практики показал, что оценка относимости электронного доказательства связывается с получением следователем, дознавателем ответов на два взаимосвязанных вопроса: 1) относится ли устанавливаемый с помощью электронного доказательства факт к

[263] Егорова Т. З. Средства доказывания и их оценка в судебных стадиях российского уголовного процесса: дис. … канд. юрид. наук. Ижевск, 2003. С.71

обстоятельствам, подлежащим доказыванию или позволяет он проверить другие доказательства; 2) способно ли данное электронное доказательство исходя из своего содержания и происхождения установить факт, подлежащий доказыванию по уголовному делу.

Между тем распространенными в следственной практике являются ошибки, допускаемые следователями, дознавателями при оценке относимости электронных доказательств. Они выражаются в подмене критерия относимости субъективным восприятием субъектом расследования схожести электронных сведений об обстоятельствах преступления, согласованных с версией обвинения, при отсутствии объективной связи рассматриваемых сведений с обстоятельствами, подлежащими доказыванию по ст. 73 УПК РФ. Электронные сведения в таких случаях не подтверждают содержание элементов предмета доказывания, но имеют значение для проверки иных доказательств по уголовному делу, установления источника иных сведений, механизма события, имеющего значение для уголовного дела. Следователи руководствуются убеждением о том, что если переписка, изображение тематически похожи на исследуемое событие (обсуждение денег, упоминание товара, разговор о встрече), то она автоматически имеет отношение к уголовному делу. Однако без установления участников коммуникации, времени и контекста взаимодействия такая похожесть нередко оказывается ошибочной. Так, при расследовании уголовного дела о мошенничестве в основу версии следователем была положена переписка из телефона потерпевшего, где обсуждалась передача денежных средств. Позднее в ходе расследования выяснилось, что переписка связана с другим контрагентом и с иными договорными отношениями, совпадение же суммы и содержание переписок носило случайный характер. Процессуальная ошибка возникла из-за отсутствия проверки следователем контакта, временных параметров, привязки к событию, обнаруженных электронных сведений[264].

[264] Материалы уголовного дела № 11901460030000704. СО по г. Подольск ГСУ СК России по Московской области.

Отсутствие в УПК РФ специальных норм, регламентирующих порядок проверки и оценки электронных доказательств, существенно осложняет их использование в уголовном судопроизводстве.

В целях преодоления обозначенных проблем представляется необходимым дополнить ст. 88 УПК РФ частью 1.1, предусматривающей, что при оценке электронных доказательств подлежат установлению их относимость не только в части содержания, но и в части наличия связи с обстоятельствами расследуемого события по техническим параметрам (сведения о дате и времени создания, изменения, передачи, получения и удаления электронных данных; метаданные электронных сведений; идентификаторы электронного устройства и носителя информации; сетевые идентификаторы и параметры соединения; сведения об учетной записи пользователя; данные о местоположении электронного устройства; контрольные значения, подтверждающие целостность электронных данных; сведения о программной среде их создания и использования; журналы событий информационной системы; а также сведения об условиях фиксации, изъятия, копирования, хранения и наличии признаков модификации электронных данных), допустимость оценивается с точки зрения законности получения и соблюдения порядка закрепления электронных доказательств, достоверность определяется посредством установления целостности, аутентичности, отсутствия признаков изменения электронных доказательств. Соответствующие предложения отражены в законопроекте по совершенствованию УПК РФ[265].

На основании изложенного можно сформулировать следующие выводы.

1. Проверка электронных доказательств на стадии предварительного расследования, предшествующая их оценке, создающая создает условия и основания для формирования обоснованных выводов об их доказательственном значении. Проверка электронных доказательств предполагает установление и анализ не только их содержания, но и процессуальной формы закрепления таких доказательств, что обеспечивает возможность проверки их происхождения, целостности, неизменности, достоверности.

[265] Приложение № 1 к диссертации.

2. Качественной проверке и оценке электронных доказательств, прежде всего их временных характеристик, препятствует неучет субъектом расследования необходимости четкого разграничения локально хранящихся электронных данных от электронных сведений, получаемых посредством удаленного доступа из облачной инфраструктуры, неверная интерпретация метаданных электронных сведений, недостоверное установление источника происхождения электронных сведений, механизма их формирования, условий актуализации и др., влекущие признания электронных доказательств недопустимыми.

3. Присущие электронным доказательствам особые признаки, отличительные свойства обусловливают необходимость дополнения ст. ст. 74, 87, 88, 164 и 177 УПК РФ предписаниями, уточняющими процедуру проверки относимости, допустимости, достоверности указанных доказательств, их последующей оценки, что обеспечит законность при установлении фактических обстоятельств в условиях цифровизации.

Глава 3. Осуществление судом проверки и оценки электронных доказательств по уголовным делам

Уголовное судопроизводство является деятельностью публичного характера, направленной на защиту интересов общества и государства. Именно поэтому судебное разбирательство предполагает открытое исследование уголовно-процессуальных доказательств, позволяющее сформировать общественное убеждение в законности и обоснованности вынесенного судебного решения[266]. Интенсивная цифровизация общественных отношений обусловила необходимость рассмотрения судом уголовных дел, доказательственная база которых формируется все чаще с помощью электронных доказательств. В данной связи Т. К. Рябинина, Д. О. Чистилина отмечают, что современная модель уголовного судопроизводства вынуждена подстраиваться под изменяющиеся условия доказательственной деятельности с учетом стремительного развития цифровых технологий, которые одновременно упрощают и усложняют в техническом плане работу сотрудников правоохранительных органов и судов[267].

Действующая модель уголовно-процессуального доказывания исторически создавалась, ориентируясь на материальные носители информации, что предопределяет использование в современной судебной практике привычных способов проверки и правил оценки уголовно-процессуальных доказательств. Указанное обстоятельство актуализирует потребность учета судом в процессе исследования электронных доказательств специфики последних, обусловленной их сущностью, отличительными свойствами.

---

[266] Марковичева Е. В., Рябинина Т. К. Гласность судебно го разбирательства по уголовным делам: баланс публичных и частных интересов // Правосудие/Justice. 2024. Т. 6. № 4. С. 132-150.

[267] Рябинина Т. К., Чистилина Д. О. Использование цифровых технологий в ходе судебного разбирательства по уголовному делу: проблемы и перспективы // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2025. №. 3 (104). С. 301.

Одним из общих условий судебного разбирательства является непосредственность, распространяющая свое действие и на процесс исследования уголовно-процессуальных доказательств. В научной литературе по этому поводу уточняется, что суд, осуществляя правосудие по уголовным делам, обязан непосредственно исследовать в судебном заседании каждое из представленных доказательств и их совокупность[268]. Действие принципа уголовного судопроизводства – свобода оценки доказательств, предусматривающее оценивание судом доказательства на основе закона и внутреннего убеждения, предоставляет судье возможность сформировать собственное мнение по результатам исследования доказательств, не связывая его с выводами, сделанными на этапе предварительного расследования[269]. Отдельно подчеркнем, что в разъяснениях Верховного Суда Российской Федерации применительно к постановлению приговору акцентируется внимание на обязанность суда оценивать все доказательства по уголовному делу, как уличающие, так и оправдывающие подсудимого, и изложить мотивы принятия одних доказательств и отклонения других[270]. Данная правовая позиция не только не теряет значение для суда при оценивании им электронных доказательств, а усиливается в рассматриваемом случае, поскольку возникает необходимость исследования специальных критериев допустимости анализируемых доказательств.

Несмотря на это**,** неучет специальных критериев допустимости электронных доказательств является одной из основных проблем современной судебной практики. В судебном разбирательстве обозначенные доказательства оцениваются с точки зрения их соответствия требованиям относимости, допустимости, достоверности и достаточности. Однако электронные сведения, содержащиеся в

---

[268] Рябинина Т. К. И вновь к вопросу об активной роли суда в уголовном судопроизводстве // Тенденции уголовной политики России на современном этапе развития общества: сборник статей Всероссийской научно-практической конференции, посвящённой 25-летию кафедр уголовного права и криминологии, уголовного процесса и правоохранительной деятельности. Ижевск, 2024. С. 65.

[269] Карякин Е. А, Миронов В. К вопросу о взаимосвязи достоверности с иными свойствами доказательств // Уголовное право. 2004. № 3. С. 85-86.

[270] Постановление Пленума Верховного Суда Российской Федерации от 29 ноября 2016 года № 55 «О судебном приговоре» // СПС «КонсультантПлюс» (дата обращения: 02.04.2025).

доказательстве, обладают специфическими свойствами: они могут легко копироваться, изменяться без очевидных визуальных следов, а отдельные их параметры зависят от программной среды и технических характеристик устройства. Именно последние определяют порядок создания, отображения, преобразования, передачи и хранения электронных данных, включая формирование метаданных, фиксацию даты, времени и геолокации, качество аудио- и видеофайлов, а также возможность выявления следов редактирования или иного вмешательства в содержание электронных сведений. Судом данные особенности нередко игнорируются.

В судебном следствии электронные доказательства необоснованно оцениваются по тем же критериям, что и доказательства, имеющие материальное происхождение. Отмеченное подтверждается судебной практикой. Так, в определении Восьмого кассационного суда общей юрисдикции от 23.12.2020 по делу № 77-3148/2020 уточнено, что электронная информация, извлеченная из цифровых носителей, не образует самостоятельного вида доказательства, требующего особых правил его оценки. Суд подчеркнул, что к таким сведениям применяются общие критерии проверки и оценки, закрепленные в статьях 87 и 88 УПК РФ. При этом суд обозначил, что электронная форма существования информации требует более тщательной проверки условий ее получения и сохранности, но она сама по себе не изменяет установленной законом модели доказательственной оценки[271].

Однако специфика электронных доказательств обуславливает необходимость учитывать целый комплекс их технических характеристик, обозначенных выше. Без анализа указанных характеристик невозможно установить подлинность и целостность электронных сведений, в отсутствие чего правильно установить фактические обстоятельства преступления и принять

[271] Кассационное определение Восьмого кассационного суда общей юрисдикции от 23 декабря 2020 года по делу № 77-3148/2020 // ГАС «Правосудие» (дата обращения: 15.01.2026).

законное и обоснованное решение. На последнее обстоятельство обращал внимание и А. В. Победкин[272].

Электронные сведения могут включать переписку в мессенджерах и социальных сетях, данные геолокации, сведения интернет-сервисов, электронные документы, аудио- и видеозаписи, а также иные формы электронной информации. Особенности получения и закрепления таких сведений часто вызывают сомнения в их достоверности, допустимости, поэтому требуют тщательной проверки судом, что отмечают М. А. Баранова, М. Д. Мишкина[273].

Анализируемая проблема усугубляется тем, что суды нередко подменяют проверку электронного доказательства формальной констатацией соблюдения процессуального порядка его получения. М. И. Воронин в данной связи указывает, что оценка судом электронных доказательств часто осуществляется по общим правилам, без учета их уязвимости к изменению по содержанию и форме, что не гарантирует достоверности электронного доказательства. В указанных целях, по мнению ученого, должна проводиться проверка его неизменности и источника происхождения[274].

Анализ уголовно-процессуальный практики свидетельствует о том, что суд признает доказательство допустимым, обосновывая свое мнение наличием протокола осмотра предметов, не исследуя при этом, насколько полно в нем отражены обстоятельства извлечения электронной информации, обеспечена ли сохранность электронных данных, исключена ли подмена устройства или файла, установлены ли временные и контекстные параметры электронных сведений, что подтверждается анализом апелляционного определения Свердловского областного суда от 24.11.2022 по уголовному делу № 22-9081/2022. В уголовном

---

[272] Победкин А. В. Публичность уголовного судопроизводства и ее отражение в доказательственном праве // Труды Академии управления МВД России. 2018. № 4 (48). С. 135.

[273] Баранова М. А., Мишкина М. Д. Проблемы аутентификации цифровых доказательств: исследование методов проверки подлинности электронных писем в суде // Государственно-правовые явления: история и современность (ко Дню Российской науки) : сборник научных статей Всероссийской научно-практической конференции. Саратов, 2025. С. 21.

[274] Воронин М. И. Недопустимая допустимость электронных доказательств. Судебная практика и пробелы в УПК // Уголовный процесс. 2020. № 10. С. 46-55.

деле электронные сведения (фотография места закладки наркотическое средства, сведения о получении координат/сообщений, использовании интернета) имели ключевое значение для доказывания направленности умысла подсудимого на приобретение наркотического средства и связи его действий с конкретным тайником. Апелляционная инстанция отменила приговор по этому уголовному делу, постановленный Верх-Исетским районным судом г. Екатеринбурга, указав на отсутствие оценки существенных несоответствий в содержании электронных сведений. Так, согласно рапорта должностного лица органа внутренних дел задержание было осуществлено в 16 часов 00 минут, а на фотографии, обнаруженной в телефоне, был указано время 19 часов 04 минуты (то есть после задержания). Другое несоответствие сведений, отраженных в материалах уголовного дела, фактической обстановке места происшествия заключалось в том, что согласно протокола осмотра места происшествия наркотическое средство было обнаружено ранней весной в сугробе, однако на фотографии в телефоне изображены признаки другого времени (земля, трава, ветки деревьев). Кроме указанного в протоколе осмотра телефона указана дата создания файла, а на представленных суду изображениях дата отсутствует. Суд первой инстанции, не разрешив сомнение в достоверности доказательств и не обосновав в своем решении, почему электронным сведениям можно доверять для установления фактических обстоятельств, допустил тем самым процессуальное нарушение – неполноту судебного разбирательства и недостаточность мотивирования судебного решения[275]. Таким образом, суд первой инстанции не должен оставлять без оценки сомнения и противоречия в исследуемых обстоятельствах, если электронное доказательство играет существенную роль для защиты подсудимого от обвинения.

Следовательно, при наличии противоречий между материальным и электронным доказательствами суд обязан установить причины таких

[275] Апелляционное определение судебной коллегии по уголовным делам Свердловского областного суда от 25 ноября 2022 года по делу №22-9081/2022 // ГАС «Правосудие» (дата обращения: 15.01.2026).

противоречий либо мотивированно объяснить, почему они не влияют на достоверность доказательства.

В апелляционном постановлении Верховного Суда Республики Калмыкия от 29.01.2020 по уголовному делу суд признал недопустимым электронное доказательство – DVD-R диск с видеозаписью гласного оперативно-розыскного мероприятия, в ходе которого обследовалось транспортное средство обвиняемого. Основанием для такого вывода послужило отсутствие в материалах уголовного дела сведений о порядке копирования видеозаписи со смартфона сотрудника ФСБ, ее передаче в подразделение полиции и надлежащем процессуальном приобщении к материалам оперативно-розыскной деятельности и уголовного дела. Суд указал, что результаты оперативно-розыскной деятельности могут использоваться в доказывании только при соблюдении требований, позволяющих установить происхождение электронных сведений и проследить законность их получения[276]. Поскольку обозначенные требования не были обеспечены, то видеозапись была исключена из числа уголовно-процессуальных доказательств, а вместе с ней и производные доказательства – протоколы ее осмотра. Данная позиция суда подтверждает, что допустимость электронного доказательства обусловлена не только его содержанием, но и документально подтвержденной сохранностью, идентифицируемостью источника и прозрачностью всей процедуры обращения электронной информации.

Неучет судом отличительных свойств электронных доказательств, специальных критериев их допустимости повышает вероятность судебных ошибок. Неполное исследование электронных сведений и отсутствие мотивированной оценки их достоверности нередко становятся основаниями для отмены судебных решений в апелляционном (ст. 389.15 УПК РФ) или кассационном (ст. 401.15 УПК РФ) порядке, что приводит к затягиванию

[276] Апелляционное постановление судебной коллегии по уголовным делам Верховного Суда Республики Калмыкия от 29 января 2020 года по делу № 22-23/2020 // ГАС «Правосудие» (дата обращения: 11.05.2026).

уголовного судопроизводства, снижению эффективности правосудия, нарушению права на доступ к справедливому правосудию в разумный срок.

Изучение практики придания судами электронным доказательствам в ходе судебного следствия юридической силы[277] свидетельствует о ненадлежащем распоряжении судом своим полномочием по проверки обозначенных доказательств. В отличие от стадии предварительного расследования, где следователь, дознаватель по ряду причин нацелен на формирование обвинительной версии по уголовному делу, судебное разбирательство предполагает полную, всестороннюю, объективную проверку судом всех доказательств, представленных сторонами уголовного процесса. Это предполагает проявление судом процессуальной активности при исследовании обозначенных доказательств, проявляющаяся в инициировании им проведения необходимых процессуальных действия для обеспечения объективной оценки собранных по уголовному делу доказательств, их достаточности для принятия правосудного итогового процессуального решения. Вместе с тем чрезмерная инициативность суда способна породить сомнения в его беспристрастности, если суд начинает подменять стороны в собирании, представлении сведений, документов, имеющих значение для уголовно-процессуального доказывания. В этой связи требуется уточнение, как верно отмечали Т. К. Рябинина, С. А. Шейфер, А. А. Плашевская, роли суда таким образом, чтобы он мог эффективно обеспечивать законность и справедливость разбирательства, не выходя за пределы своего нейтрального процессуального статуса[278]. По мнению

[277] Кассационное определение Второго кассационного суда общей юрисдикции от 21 января 2025 года № 77-109/2025; Кассационное определение Второго кассационного суда общей юрисдикции от 18 декабря 2025 года № 77-3391/2025; Кассационное определение Второго кассационного суда общей юрисдикции от 14 ноября 2023 года № 77-3590/2023 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

[278] Рябинина Т. К. Роль суда в обеспечении баланса частных и публичных интересов в уголовном судопроизводстве // Российское правосудие. 2022. № 2. С. 78-88; Плашевская А. А. Собирание судом доказательств при рассмотрении дела по первой инстанции в уголовном процессе России: автореф. дис. … канд. юрид. наук. Томск, 2006. С. 13-15; Васин В. В. Уголовно процессуальное познание судом первой инстанции обстоятельств уголовного дела: автореф. дис. … канд. юрид. наук. Томск, 2006. С. 7-10; Ларинков А. А. Теоретические и правоприменительные проблемы доказывания на стадии судебного разбирательства: автореф.

В. Л. Будникова, суд обязан совершать все предусмотренные законом действия, необходимые для правильного и справедливого разрешения уголовного дела по существу, одновременно гарантируя равенство процессуальных возможностей сторон при реализации их прав и исполнении обязанностей[279]. В рассматриваемом аспекте ожидания от суда осуществления действий по надлежащей проверке электронных доказательств согласуется с правовой позицией Конституционного Суда Российской Федерации, согласно которой деятельность по собиранию доказательств не является исключительной прерогативой сторон уголовного процесса. Соответствующие полномочия, по мнению Конституционного Суда Российской Федерации, принадлежат и суду, который реализует их в установленном уголовно-процессуальным законом порядке в рамках судебного следствия[280]. Поскольку согласно теории доказательственного права способами проверки доказательств является не только мыслительная деятельность уполномоченного субъекта, но и осуществление необходимых следственных и иных процессуальных действий[281], то представленная позиция Высшего суда нивелирует сомнения ученых и практических работников органов уголовной юстиции о наличии у суда процессуальной обязанности осуществлять процессуальные действия, в том числе для проверки электронных доказательств, в

дис. … канд. юрид. СПб., 2006. С. 18-19; Пиюк А. В. Роль суда в собирании доказательств по уголовному делу на стадии предварительного расследования и при рассмотрении дела в суде первой инстанции: автореф. дис. … канд. юрид. наук. Томск, 2004. С. 7-8; Шейфер С. А. О понятии и цели доказывания в уголовном процессе // Государство и право. 1996. № 9. С. 65.

[279] Будников В. Л. Субъекты обязанности доказывания в уголовном судопроизводстве // Российская юстиция. 2008. № 5. С. 27.

[280] Определение Конституционного Суда Российской Федерации от 06 марта 2003 года № 104-О «Об отказе в принятии к рассмотрению запроса Бокситогорского городского суда Ленинградской области о проверке конституционности части первой статьи 86 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 16.04.2026).

[281] Костенко Р. В. Процессуальные действия как способ проверки доказательств в уголовном судопроизводстве // Юридический вестник Кубанского государственного университета. 2020. № 3. С. 46; Рудин А. В. Основные теоретические проблемы проверки доказательств на стадии досудебного производства в уголовном процессе // Закон и право. 2018. № 3. С. 111; Гладышева О. В., Семенцов В. А. Уголовно процессуальное право. Общая часть и досудебное производство: курс лекций. Краснодар. 2011. С. 130; Сморгунова М. Е. Теоретические основы и практика проверки досудебных доказательств в уголовном процессе: дис. … канд. юрид. наук. Нижний Новгород. 2004. С. 64.

целях формирования добротной доказательственной базы по уголовному делу. В развитие указанного, научно-практический интерес представляет утверждение С. В. Рудаковой о необходимости активной и независимой познавательной позиции суда. По ее мнению, суд не должен ограничиваться доказательствами, представленными сторонами, и в целях формирования полного представления о событии преступления вправе проявлять инициативу в собирании доказательств[282], включая случаи возникновения сомнений в допустимости электронного доказательства.

Т. К. Рябинина отмечает, что суд достаточно активно участвует в проверке уголовно-процессуальных доказательств, представленных сторонами, – допрашивая подсудимых, потерпевших, свидетелей, заслушивая заключения судебных экспертов, осматривая вещественные доказательства и оглашая протоколы и документы[283]. Однако в судебной практике нередко возникают ситуации, когда суд ограничивается пассивным восприятием материалов уголовного дела, фактически дублируя выводы органов предварительного расследования по обстоятельствам, подлежащим доказыванию. Особенно отчетливо обозначенная ситуация проявляется при проверке судом электронных доказательств.

Ненадлежащая проверка электронных доказательств судом проявляется в уходе суда от непосредственного исследования электронной информации. В частности, нередко аудио- и видеозаписи, содержащиеся на электронных носителях, не воспроизводятся в судебном заседании. Суд в указанных случаях ограничивается оглашением протоколов осмотров носителей, составленных следователем, дознавателем, что не согласуется с предписаниями ст. 240 УПК РФ о непосредственности судебного разбирательства. Однако

---

[282] Рудакова С. В. Познание судом обстоятельств уголовного дела: автореф. дис. … канд. юрид. наук. Краснодар, 2004. С. 7.

[283] Рябинина Т. К. И вновь к вопросу об активной роли суда в уголовном судопроизводстве // Тенденции уголовной политики России на современном этапе развития общества : сборник статей Всероссийской научно-практической конференции, посвященной 25-летию кафедр уголовного права и криминологии, уголовного процесса и правоохранительной деятельности. Ижевск, 2024. С. 65.

Седьмой кассационный суд общей юрисдикции не усмотрел в таком порядке исследования электронных доказательств нарушений закона. В обосновании своих доводов кассационная инстанция признала данный порядок допустимым, указала на отсутствие ходатайства стороны защиты о воспроизведении записей в судебном заседании[284]. Представляется, что системное толкование общих условий судебного разбирательства и правил оценки доказательств по уголовному делу (ст. 88 УПК РФ) обуславливает избыточность требования со стороны вышестоящей судебной инстанции о заявлении обозначенного выше ходатайства стороны защиты.

Таким образом, можно сделать вывод о том, что в судебной практике допускается исследование электронных доказательств в опосредованной форме – только посредством оглашения протоколов осмотра устройств. Подобный порядок не должен рассматриваться как достаточный, оптимальный способ исследования электронных доказательств. В случаях, когда электронные сведения имеют существенное значение для установления фактических обстоятельств уголовного дела, основным способом их проверки должно выступать непосредственное воспроизведение соответствующих аудио- и видеозаписей в судебном заседании. В противном случае существует риск принятия неправосудного решения по уголовному делу.

Ненадлежащее осуществление судом своих полномочий проявляется также в непроведении им проверки происхождения электронных сведений. Для оценки доказательственного значение электронной информации суду, следуя предписаниям ст. 87 УПК РФ, необходимо установить источник ее формирования, электронное устройство или информационную систему, в которой она была создана, а также процессуальный порядок ее включения в материалы уголовного дела. Однако анализ судебной практики показывает, что нередко такие обстоятельства остаются невыясненными судом либо фиксируются в протоколе судебного заседания неполно, что ставит под сомнение подлинность и

[284] Кассационное определение Седьмого кассационного суда общей юрисдикции от 21 июля 2021 года № 77-2749/2021 // СПС «КонсультантПлюс» (дата обращения: 02.04.2025).

неизменность электронных доказательств. Данный факт подтверждает и А. Н. Бачило, указывая на причины возникающего сомнения – из-за возможного изменения цифровых следов, отсутствия сертифицированных методов проверки и сложности установления достоверности метаданных. Это, по мнению ученого, подразумевает необходимость тщательного изучения происхождения и целостности электронных данных[285]. Обобщение результатов уголовно-процессуальной практики свидетельствует, о том, что не установление генезиса происхождения электронных сведений нередко становится основанием для признания таких доказательств недопустимыми и, как следствие, влечет их исключение из системы доказательств по уголовному делу. Так, кассационные суды делают выводы о признании недопустимым доказательством видеозапись, если неясно, как она появилась в материалах уголовного дела, кем и когда была приобщена, почему отсутствует в материалах проверки сообщения о преступлении, и какими процессуальными действиями обеспечена ее сохранность[286].

Использование судом производных форм электронной информации – скриншотов, фототаблиц, распечаток переписки в судебном следствии также свидетельствует о недостаточной активности суда при проверке электронных уголовно-процессуальных доказательств. Подобные материалы широко используются в уголовно-процессуальном доказывании, однако они часто не содержат необходимых сведений о времени их создания, контексте сообщения или источнике получения электронной информации. При отсутствии доступа к первоначальному источнику электронной информации, производные формы электронной информации практически не поддаются проверке на достоверность, что существенно снижает их доказательственную ценность. Так, Наро-Фоминский

---

[285] Бачило А. Н. Достоверность электронных доказательств: проблемы верификации // Вестник цифрового права. 2019. № 3(12). С. 45-52.

[286] Кассационное определение Первого кассационного суда общей юрисдикции от 09 января 2021 года № 77-3490/2021; Кассационное определение Первого кассационного суда общей юрисдикции от 25 ноября 2020 года по делу №77-2301/2020; Кассационное определение Третьего кассационного суда общей юрисдикции от 01 сентября 2020 года по делу № 77-870/2020 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

городской суд Московской области исследовал протокол личного досмотра Б., согласно которого у Б. был обнаружен и изъят мобильный телефон. Каких-либо действий, связанных с его разблокировкой или его включением в протоколе личного досмотра не отражено. При этом, к протоколу личного досмотра в качестве приложения следователем была приобщена фототаблица, из содержания которой не было ясно, каким образом были получены скриншоты переписки. Внешний вид мобильного телефона отличался от устройства, на котором якобы был изображен скриншот: наличие на верхней части мобильного телефона несколько круглых точек, отсутствовавших на устройстве, в котором обнаружены скриншоты; отличие размера дисплея мобильного телефона от дисплея, на котором были обнаружены скриншоты. Суд в приговоре при оценке допустимости обозначенного доказательства ограничился указанием на соблюдение порядка его получения – в соответствии с требованиями УПК РФ, а также исследования в ходе судебного разбирательства[287]. В данном случае протокол следственного действия и приложенная к нему фототаблица со скриншотами переписки не могут расцениваться как достоверное подтверждение генезиса происхождения электронных сведений. Доказательственное значение таких материалов возникает лишь при установлении источника их формирования, конкретного электронного носителя информации и условий фиксации соответствующих электронных сведений. Суд должен стремиться к исследованию первоначального источника электронного доказательства или при невозможности указанного привлекать специалиста для проведения полной и качественной проверки происхождения и неизменности электронного доказательства.

Представленная практика проверки судом электронных доказательств приводит к снижению надежности доказательственной базы по уголовному делу. Суд фактически оценивает не содержание электронной информации и ее происхождение, а лишь визуальное отображение такой информации, что не

[287] Приговор Наро-Фоминского городского суда Московской области от 15 января 2025 года по делу № 1-13/2025. ГАС «Правосудие» (дата обращения: 05.05.2026).

отвечает требованию достоверности, предъявляемому к уголовно-процессуальному доказательству.

Негативные последствия приведенной судебной практики влекут формирование недостаточно проверенной на соответствие закону доказательственной базы по уголовному делу, обоснование судом выводов по результатам судебного разбирательства сведениями, происхождение и достоверность которых не установлены должным образом. В таких условиях повышается риск допущения судебных ошибок при отправлении правосудия по уголовному делу, нарушения прав участников уголовного судопроизводства, гарантированных УПК РФ

Решения обозначенной проблемы видится в закрепление в уголовно-процессуальном законе требования о необходимости непосредственного исследования электронных доказательств в судебном заседании. Учитывая действие общего условия судебного разбирательства – непосредственность, представляется целесообразным дополнить статью 240 УПК РФ частью первой.1, содержащей предписание о том, что при исследовании доказательств по уголовному делу, содержащих электронные сведения, суд при наличии технической возможности обеспечивает воспроизведение аудио- и видеозаписей, демонстрацию электронных файлов либо исследование электронного носителя информации или его цифрового образа. Изучение протоколов осмотра предметов и иных производных объектов должно расцениваться судом как дополнительный способ исследования уголовно-процессуальных доказательств. Учитывая значимость установления происхождения электронных сведений для придания им доказательственного значения по уголовному делу, суду для надлежащей оценки таких сведений необходимо устанавливать источник их формирования, условия получения и процессуальный порядок приобщения обозначенных сведений к материалам уголовного дела. В этой связи представляется целесообразным закрепить соответствующие требования в статье 87 УПК РФ[288].

[288] Приложение № 1 к диссертации.

Раскрывая особенности проверки и оценки судом уголовно-процессуальных доказательств, следует акцентировать внимание на ограничение конституционного принципа состязательности и равноправия сторон (ч. 3 ст. 123 Конституции РФ) при представлении и исследовании доказательств в судебном разбирательстве. Положения данного принципа презюмируют равные процессуальные возможности стороны обвинения и защиты в представлении и исследовании доказательств, предшествующих принятию судом итогового решения по уголовному делу, а также беспристрастность суда при оценке доказательств независимо от того, позицию какой стороны они подтверждают. С учетом изложенного суд обязан обеспечивать равные условия для осуществления сторонами своих процессуальных прав и не допускать создания преимуществ одной из сторон при исследовании доказательств. На данное правило проверки уголовно-процессуальных доказательств указал Верховный Суд Российской Федерации[289]. Однако анализ судебной практики свидетельствует о фактах неравного подхода судов к проверке и оценке электронных доказательств – в зависимости от субъекта уголовного процесса, их представляющего. Вместе с тем М. Б. Набатов указывает, что современному российскому правоприменению не хватает не состязательности как таковой, а равноправия сторон, особенно в части, касающейся участия профессионального адвоката в процессе доказывания[290].

В условиях цифровизации общественных отношений электронные сведения все чаще используются как стороной обвинения, так и стороной защиты для обоснования своей позиции по уголовному делу. Справедливо отмечает М. Б. Набатов, что адвокат – единственный профессиональный участник на стороне защиты, равный по профессиональной подготовке властным субъектам,

---

[289] Постановление Пленума Верховного Суда Российской Федерации от 19 декабря 2017 года № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)» // СПС «КонсультантПлюс» (дата обращения: 17.04.2025).

[290] Набатов М. Б. Реализация права на защиту в уголовном процессе в условиях применения цифровых технологий : автореф. … дис. канд. юрид. наук. М., 2024. С. 16.

он обязан быть более активным участником доказывания, что требует расширения не только его полномочий, но и предоставления ему технических возможностей[291].

В нередких случаях электронные сведения, представленные стороной обвинения, признаются судом допустимыми при их формальной проверке, тогда как аналогичные по форме материалы стороны защиты отклоняются судом по причине невозможности установить их происхождение, чем нивелируется процессуальная форма получения электронного доказательства. Подобная судебная практика свидетельствует о необоснованном ограничении действия принципа состязательности и равноправия сторон в уголовном судопроизводстве, поскольку электронные доказательства, представленные стороной обвинения, для суда имеют юридическую силу, в том числе презюмируются как отвечающие свойствам достоверности, в отличие от электронных материалов, представленных стороной защиты – они заведомо являются недопустимыми. Подтверждением указанного выступает ходатайство следователя перед судом об избрании меры пресечения в виде заключения под стражу. Стороной защиты были представлены суду скриншоты интернет-сервиса бронирования гостиничного номера на паспортные данные обвиняемого Я., подтверждающие его намерение находиться по конкретному адресу в определенный период времени. Однако суд отказался приобщить указанные электронные сведения к материалам производства, сославшись на невозможность достоверно установить их происхождение[292]. При этом суд не предпринял каких-либо действий, направленных на проверку представленных сведений, хотя имел возможность истребовать необходимую информацию у соответствующего интернет-сервиса, мог бы предложить сторонам представить дополнительные доказательства в подтверждении своих доводов по исследуемому вопросу.

Подтверждение ограничения состязательности и равноправия сторон в представлении участниками судебного разбирательства электронных сведений

---

[291] Набатов М. Б. Указ. раб. С. 9.

[292] Постановление Адлерского районного суда г. Сочи Краснодарского края от 19 июня 2024 года по делу № 3/1-115/2024 // ГАС «Правосудие» (дата обращения: 17.04.2025).

для отстаивании правовой позиции находит и в кассационном определении Первого кассационного суда общей юрисдикции от 07.10.2025 по делу № 77-3195/2025 по уголовному делу в отношении П., в котором сторона защиты ссылалась на видеозапись на оптическом диске, содержащую момент рубки лесных насаждений, как на электронное доказательство, подтверждающее невиновность осужденного. Адвокат указывал, что видеозапись содержит сведения, ставящие под сомнение версию стороны обвинения относительно места, характера и обстоятельств незаконной рубки, в частности ссылалась на особенности геоданных и на несоответствие зафиксированной на записи обстановки описанию инкриминированного деяния. Однако суд исключил данную видеозапись из числа доказательств как не имеющую отношения к уголовному делу, а кассационная инстанция признала такое решение законным[293]. Тем самым суд фактически отказался придать электронным сведениям, представленным стороной защиты, самостоятельное доказательственное значение, несмотря на доводы о необходимости дополнительной проверки их технических характеристик и происхождения. Данный пример судебной практики показывает, что электронные сведения, представляемые стороной защиты, судом, как правило, оцениваются более строго, чем электронные материалы, представленные стороной обвинения, что демонстрирует нарушение принципа состязательности и равноправия сторон, противоречит требованиям Основного закона. Предъявляя повышенное внимание к достоверности, допустимости электронных материалов, представленных стороной защиты, но не действуя аналогичным образом при проверке к доказательствам, представленных стороной обвинения, суд тем самым создает неравные условия участия в уголовном процессе. С точки зрения теории доказывания подобный подход суда способен привести к формированию так называемой «асимметрии доказательств», при которой сведения, представленные стороной обвинения, оцениваются судом как более надежные и значимые для установления фактических обстоятельств по

[293] Кассационное определение Первого кассационного суда общей юрисдикции от 07 октября 2025 года № 77-3195/2025 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

уголовному делу, материалы же стороны защиты необоснованно признаются как ничтожные. Вследствие указанного доказательственная база по уголовному делу формируется преимущественно на основе доказательств стороны обвинения, доказательства же, представленные стороной защиты, утрачивают юридическое значение в ходе процесса доказывания. Схожее мнение высказывали Ю. П. Буруленков, В. Л. Кудрявцев [294]. В данной связи заслуживает внимания мнение Ф. М. Кудина и Р. В. Костенко о том, что содержание доказательств, вне зависимости от того, являются ли они обвинительными или оправдательными, не должно влиять на решение вопроса об их допустимости[295].

Проблема осложняется тем, что у стороны защиты меньше возможностей собрать и тем более процессуально закрепить электронные сведения в отличие от следователя, дознавателя, которые наделены полномочиями по производству следственных действий, изъятию электронных носителей информации, назначению и производству судебных экспертиз, получению сведений у операторов связи и интернет-сервисов. Сторона защиты часто располагает лишь копиями электронных данных или их визуальным отображением. В подобных условиях чрезмерно строгие требования суда к подтверждению происхождения электронных сведений могут фактически лишить сторону защиты возможности использовать электронную информацию в качестве доказательства по уголовному делу. М. Б. Набатов в этих случаях предлагает следующее решение – для достижения равенства между стороной обвинения и защиты, особенно в вопросах, касающихся процесса доказывания, предусмотреть официальное оформление ввода защитником в материалы уголовного дела доказательственной информации, которая не может быть не принята или уничтожена следователем[296]. По этому поводу О. Е. Жамкова уточняет, что в уголовно-процессуальной науке

[294] Боруленков Ю. П. Допустимость доказательств: время перемен? // Уголовное судопроизводство. 2013. № 3. С. 16; Кудрявцев В. Л. Проблемы двойного стандарта при определении допустимости доказательств в российской уголовно-процессуальной науке // Актуальные проблемы уголовно-процессуального права и практика его применения : материалы международной дистанционной научно-практической конференции. Караганда, 2009. С. 7-13;

[295] Кудин Ф. М., Костенко Р. В. Допустимость доказательств в российском уголовном процессе: учебное пособие. Краснодар, 2002. С. 78-79.

[296] Набатов М. Б. Указ. раб. С. 16.

сформировались две основные позиции. Согласно одной из них сведения, собранные защитником, должны автоматически признаваться доказательствами и приобщаться к уголовному делу. Суть другой позиции состоит в необходимости последующей оценки собранных защитником доказательств уполномоченным должностным лицом на предмет допустимости и достоверности[297]. Судебная практика свидетельствует о не восприятии до настоящего времени судами ни первой, ни второй инстанции.

В развитие указанного подчеркнем, что современные электронные сервисы и информационные системы часто не предусматривают простых технологических механизмов подтверждения происхождения отдельных электронных сведений. Например, скриншоты интернет-страниц, переписка в мессенджерах или данные интернет-сервисов могут не содержать всех технических атрибутов (метаданные о времени создания и изменения файла, источнике его формирования, параметрах устройства, учетной записи пользователя и иных условиях фиксации электронной информации), позволяющих без сомнения определить условия их формирования. В подобных ситуациях отказ суда в принятии таких материалов от защитника без попытки их дополнительной проверки можно расценивать как умаление роли стороны защиты в отстаивании своей позиции по уголовному делу.

Отмечающиеся в рассматриваемой судебной практике нарушения принципа состязательности и равноправия сторон в уголовном судопроизводстве обуславливают то обстоятельство, что сторона защиты оказывается в менее благоприятном положении при представлении и исследовании уголовно-процессуальных доказательств. Это может существенно ограничивать ее возможности по опровержению обвинения, вменяемого подсудимому. Наделение защитника правом собирания уголовно-процессуальных доказательств в настоящее время не реализуемо, так как отсутствуют гарантии и процессуальные

[297] Жамкова О. Е. Юридическая значимость сведений, полученных защитником по уголовному делу // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : сборник научных статей. Орёл, 2024. С. 88.

механизмы, обеспечивающие это право[298]. В результате повышается риск нарушение прав на защиту и справедливое судебное разбирательство.

Для оптимизации процедур проверки и оценки электронных доказательств суд должен использовать предусмотренные уголовно-процессуальным законом способы проверки представленных сторонами материалов: истребовать информацию у соответствующих организаций или интернет-сервисов, вызывать представителей организаций для дачи пояснений по поводу принадлежности аккаунта, условий формирования электронных сведений, времени их создания или передачи, а также порядка их хранения и выдачи по запросу, назначать судебную экспертизу либо привлекать специалиста для анализа технических характеристик электронных сведений. Применение указанных процессуальных средств позволит обеспечить объективную проверку и оценку судом электронных доказательств, не допускать необоснованного ограничения процессуальных прав сторон в судебном разбирательстве.

В качестве самостоятельной проблемы, возникающей при проверке и оценке судом электронных доказательств, следует выделить необоснованное сужение гарантий конституционных прав личности на тайну переписки, телефонных переговоров и иных сообщений (ст. 23 Конституции Российской Федерации) при использовании электронных доказательств в доказывании по уголовному делу. В уголовно-процессуальной практике допускается извлечение информации из памяти изъятого мобильного устройства в отсутствие судебного решения на такое извлечение. Осмотр переписки, находившейся в памяти электронного устройства, в отсутствии судебного решения, признается допустимым. Формированию подобной практике способствует правовая позиция Конституционного Суда Российской Федерации, который неоднократно указывал на отсутствие необходимости вынесения специального судебного решения для

[298] Гурдин С. В. Собирание и представление доказательств защитником – реальность или процессуальная иллюзия? // Криминологический журнал. 2020. № 4. С. 50; Малышева О. А. Процессуальная форма участия защитника в доказывании в досудебном производстве требует оптимизации // Актуальные проблемы российского права. 2023. Т. 18. № 5 (150). С. 123-131.

проведения осмотра изъятых абонентских устройств и судебной экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, которые изъяты при производстве следственных действий в установленном законом порядке[299]. Так, Наро-Фоминским городским судом Московской области признан допустимым доказательством протокол осмотра переписки, содержащейся в приложении WhatsApp на мобильном телефоне, изъятом в ходе производства личного досмотра гражданина Ч.[300].

По мнению Верховного Суд Российской Федерации, решение суда для производства следственных действий (контроль записи телефонных и иных переговоров, получение информации о соединениях между абонентами и (или) абонентскими устройствами) необходимо в случаях, когда может произойти нарушение тайны переписки[301]. Если переписка содержит в себе вымышленные имена, методы конспирации, и не касается личной жизни, то необходимость в получении судебного решения для производства вышеуказанных следственных действий не требуется. В связи с указанным В. В. Иванов отмечает, что фактически складывается ситуация, при которой объем гарантий прав личности на тайну телефонных переговоров и защищенность информации зависит не от ее

---

[299] Определения Конституционного Суда Российской Федерации от 25 января 2018 года № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации», от 17 июля 2018 года № 1955-О «Об отказе в принятии к рассмотрению жалобы гражданина Сидака Константина Петровича на нарушение его конституционных прав частью шестой статьи 164 и статьей 177 Уголовно-процессуального кодекса Российской Федерации», от 28 ноября 2019 года № 3205-О «Об отказе в принятии к рассмотрению жалобы гражданина Габашвили Игоря Сергеевича на нарушение его конституционных прав частью первой статьи 176 и частью второй статьи 177 Уголовно-процессуального кодекса Российской Федерации», от 24 июня 2021 года № 1364-О «Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 02.04.2025).

[300] Приговор Наро-Фоминского городского суда Московской области от 31 октября 2024 года по делу № 1-358/2024. Доступ из ГАС «Правосудие» (дата обращения: 23.03.2025).

[301] Апелляционное определение Судебная коллегия по уголовным делам Верховного Суда РФ от 01 августа 2019 года по делу № 67-АПУ19-8 // СПС «КонсультантПлюс» (дата обращения: 12.04.2025).

содержания, а от способа доступа к ней: при наличии в распоряжении следователя мобильного телефона извлечение информации, составляющей тайну переписки и переговоров, осуществляется без судебного контроля, тогда как при отсутствии устройства получение тех же сведений возможно только на основании судебного решения[302]. Данными позициями высших судов должен руководствоваться суд при рассмотрении уголовного дела по существу и принятии итогового решения.

Правовая позиция Конституционного Суда Российской Федерации уточняет пределы ограничения обозначенного права личности. Законное изъятие устройства освобождает властного субъекта от дополнительного получения разрешения суда производство осмотра электронной информации из памяти изъятого абонентского устройства и проведения судебной экспертизы, предметом исследования которой выступает указанная информация. Однако получение аналогичных сведений от операторов связи или интернет-сервисов возможно только на основании судебного решения. Для оценки судом допустимости электронного доказательства ему важно разграничить источник электронной информации – либо это память абонентского устройства, либо это коммуникационные данные у иных лиц. При извлечении переписки фактически через доступ к аккаунту / облаку возникает иной характер нарушения тайны телефонных переговоров, переписки, соединений между абонентами. Поэтому суду необходимо проверять, были ли соблюдены требования по осуществлению судебного контроля в необходимых случаях.

В теории уголовного процесса судебный контроль обычно рассматривается как многоуровневый механизм судебной защиты прав личности, включающий, во-первых, предварительный судебный контроль, осуществляемый до производства процессуального действия и выражающийся в даче судом разрешения на производство следственных и иных процессуальных действий, затрагивающих конституционных права участников уголовного

[302] Иванов В. В. Защита охраняемых законом тайн при производстве следственных действий с мобильным телефоном и иными электронными носителями информации // Правовое государство: теория и практика. 2021. № 4. С 183.

судопроизводства; во-вторых, последующий судебный контроль, реализуемый при проверке судом законности и обоснованности уже произведенных действий и принятых решений, в том числе в порядке, предусмотренном ст. 125 УПК РФ; в-третьих, судебный контроль при рассмотрении уголовного дела по существу, когда суд в ходе судебного разбирательства оценивает соблюдение требований закона при собирании доказательств и решает вопрос об их допустимости[303].

Применительно к электронным доказательствам такая многоуровневая система означает необходимость установления того, что требовалось ли предварительное судебное решение для получения соответствующих сведений, могла ли законность их получения быть предметом последующего обжалования и дана ли надлежащая итоговая оценка допустимости этих сведений при разрешении уголовного дела. Для надлежащей оценки допустимости электронных доказательств суд должен руководствоваться необходимостью разграничения локальных сведений, сведения иных лиц и серверно-облачных сведений. Не осуществление подобного разграничения ведет к ошибкам в оценке допустимости электронных доказательств и к необоснованным ограничениям конституционных прав личности.

Дополнительные сложности в доказательственной деятельности суда возникают в ситуациях, когда доступ к переписке осуществляется не из памяти устройства, а через аккаунты пользователей или облачные хранилища и различные интернет-сервисы, в том числе электронную почту, мессенджеры, социальные сети, личные кабинеты интернет-платформ, файлообменные сервисы, сервисы резервного копирования и иные удаленные информационные ресурсы. Различные виды доступа к электронной информации предусмотрены

[303] Ласточкина Р. Н., Язева Е. Е., Кулев А. Г. Судебный контроль в уголовном процессе: учебно-методическое пособие. Ярославль: ЯрГУ, 2017. С. 6; Русман Г. С. Судебный контроль за применением мер пресечения в виде заключения под стражу, домашнего ареста: автореф. …дис. канд. юрид. наук. Челябинск, 2011. С. 6; Адильшаев Э. А. Судебное санкционирование в уголовном процессе России: автореф. … дис. канд. юрид. наук. Ижевск, 2011. С. 9; Муратова Н. Г. Система судебного контроля в уголовном судопроизводстве: вопросы теории, законодательного регулирования и практики: автореф. … дис. д-ра юрид. наук. Екатеринбург, 2004. С. 9.

Федеральным законом от 07.07.2003 № 126-ФЗ «О связи»[304], а также Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[305]. В таких случаях субъект расследования обращается к электронным данным, размещенным на удаленных серверах, что требует особого порядка судебного контроля. Аналогичной позиции придерживается В. Е. Смирнов, указывая на обязательное получение судебного решения для извлечения и осмотра электронной информации с подобных цифровых устройств[306]. Без акцентирования внимания судом на различные источники электронной информации – память электронного устройства, данные операторов связи, облачные сервисы, возникает риск нарушения конституционного права на неприкосновенность частной жизни. Связь между правом на неприкосновенность частной жизни и тайной переписки заключается в том, что последняя выступает одной из конституционно-правовых гарантий защиты частной жизни. Поэтому доступ к электронным сообщениям, сведениям о соединениях, аккаунтам и облачным данным затрагивает не только содержание коммуникации как таковой, но и частную сферу личности в целом, что требует особенно строгой проверки законности получения таких сведений и соблюдения судебного порядка ограничения соответствующих прав[307]. Кроме того, собирание без учета обозначенных выше правил электронного доказательства, презюмирует его непригодность для доказывания по уголовному делу.

---

[304] Федеральный закон от 07 июля 2003 года № 126-ФЗ «О связи» // СПС «КонсультантПлюс» (дата обращения: 02.04.2026).

[305] Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс» (дата обращения: 02.04.2026).

[306] Смирнов В. Е. Гарантии прав личности в уголовном судопроизводстве в условиях цифровизации : автореф. … дис. канд. юрид. наук. М., 2025. С. 25.

[307] Соколов А. Б., Третьякова Е. И. Осмотр мобильного телефона: неразрешенные вопросы правоприменения // Криминалистика: вчера, сегодня, завтра : сборник научных трудов Иркутск : Восточно-Сибирский институт МВД России. 2023. Т. 26. № 2. С. 223-224; Бычков В. В. Соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при проверке сообщений о преступлениях и в ходе их расследования // Российский следователь. 2013. № 24. С. 11.

Дополнительным элементом правового регулирования получения и использования электронных доказательств в уголовном судопроизводстве может стать закрепление обязанности органов предварительного расследования указывать в процессуальных документах о признании доказательством источник получения электронной информации и характер доступа к ней. Это позволит суду при оценке электронных доказательств установить, получены ли сведения из памяти устройства, от операторов связи либо из удаленных информационных систем, и определить необходимость судебного решения для их получения, поскольку различный источник электронной информации предполагает различный правовой режим доступа к ней и разные пределы ограничения конституционного права личности.

Таким образом, в качестве процессуальной гарантии правильной оценки судом электронного доказательства, исключающей необоснованное ограничение конституционного права личности на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также на неприкосновенность частной жизни**,** следует рассматривать возложение на следователя, дознавателя процессуальных обязанностей отражения в протоколе следственного действия при извлечения электронной информации способа, источник получения этой информации.

Раскрытие проблем, возникающих в связи с проверкой и оценкой судом электронных уголовно-процессуальных доказательств, и носящих процессуальный характер, целесообразно осуществлять во взаимосвязи с материально-техническим обеспечением судебной деятельности. У суда при исследовании электронных доказательств возникают объективные сложности, обусловленные недостаточной технической оснащенностью судов общей юрисдикции. На данную проблему обращает внимание и А. Ф. Волынский[308]. Как отмечает ученый, в отличие от органов предварительного расследования,

[308] Волынский А. Ф. Научно-техническое обеспечение судопроизводства: привычные проблемы и программно-целевой подход к их решению // Известия Тульского государственного университета. Экономические и юридические науки. 2023. № 2. С. 3-12.

располагающих специализированными программно-техническими средствами для извлечения, анализа и фиксации электронной информации, суды часто не обладают необходимой инфраструктурой для полноценной работы с электронными носителями и цифровыми данными. Это проявляется в отсутствии программного обеспечения для анализа цифровых файлов, а также защищенных систем, позволяющих безопасно воспроизводить электронные материалы в судебном заседании. На необходимость размещения в помещениях судов современного технологического оборудования обращала внимание и Н. П. Гололобова[309]

В настоящее время в судах отсутствует безопасная среда для воспроизведения электронных носителей информации. Использование обычных компьютеров при исследовании файлов, полученных с внешних носителей, может создавать риск заражения вредоносным программным обеспечением, утечки конфиденциальных данных или несанкционированного доступа к информационным системам суда. В условиях отсутствия изолированной цифровой среды суды нередко избегают непосредственного открытия файлов с носителей, ограничиваясь их распечатками или описанием в протоколах следственных действий. Это первая составляющая проблемы организационно-правового характера, препятствующей надлежащей проверке и оценке доказательств. Другая составляющая обозначенной проблемы связана с отсутствием единого стандарта оборудования и программного обеспечения, используемого судами для воспроизведения электронных доказательств. Электронная информация может существовать в различных форматах – текстовых, аудио-, видео-, графических, а также в виде специализированных отчетов программ извлечения данных из мобильных устройств. Для корректного воспроизведения таких материалов требуется соответствующее программное

[309] Гололобова Н. П. Использование современных средств связи для оптимизации рассмотрения уголовных дел в суде: Уголовный процесс и прокурорский надзор: национальные стратегии, практики, инновации // Выступление на международной научно-практической конференции 3 апреля 2026 г. Кубанский госуниверситет. Краснодар, 2025. 03 апр.

обеспечение и технические средства, которые в судах часто отсутствуют. Это приводит к ситуации, когда даже при наличии электронных файлов суд не имеет возможности их полностью просмотреть и исследовать в судебном заседании.

Указанные выше составляющие проблемы всестороннего, полного объективного исследования электронного доказательства и его оценки препятствуют непосредственному исследованию первоначального источника электронной информации. В большинстве случаев перед судом стоит задача проверить не само электронное устройство или исходный файл, а лишь с производные материалы от электронных сведений – распечатки переписки, фототаблицы, скриншоты или протоколы следственных действий. При этом суд не имеет возможности самостоятельно проверить такие параметры электронного доказательства, как структура файла, метаданные, системное время устройства, хронологическая последовательность сообщений или иные технические характеристики, которые могут иметь существенное значение для определения достоверности доказательства.

Специалистами в области цифровых технологий обращается внимание на наличие системных инфраструктурных ограничений, препятствующих полноценному использованию рассматриваемых технологий в деятельности судов. В частности, отмечается отсутствие единого цифрового контура в судах. Максимальный износ значительной части используемого серверного оборудования, функционирование основных информационных решений, используемых в работе судов (включая ГАС «Правосудие») на устаревших импортных версиях программного обеспечения, не имеющих аттестатов соответствия по требованиям информационной безопасности[310]. Приведенные факты подтверждают суждения соискателя о неготовности суда к использованию электронных доказательств для установления обстоятельств, имеющих значение для уголовного дела, с применением особых правил, обусловленных

[310] Не в цифре – Счетная палата оценила состояние информатизации судебной системы [Электронный ресурс]. URL: https://ach.gov.ru/checks/ne-v-tsifre(дата обращения: 17.04.2026).

специальными критериями допустимости этих доказательств, специфических технологий для исследования последних.

Существующие технические и программные ограничения влияют на возможности судов работать с электронной информацией, включая с электронными доказательствами. Вместе с тем в научной литературе обращается внимание на риски технического характера, возникновение которых связывается с цифровизацией судебного процесса. В данной связи отмечается, что «технические сбои электронных сервисов, нестабильный уровень интернет-соединения, неисправность аудио- или видеоустройств могут существенно влиять на возможность восприятия сторонами и оценки судом доказательств»[311]. Подобные обстоятельства способны затруднить демонстрацию электронных материалов в судебном заседании и ограничивать возможности сторон по их анализу. В результате исследование доказательств нередко сводится к ознакомлению с протоколами следственных действий и распечатками электронных материалов, что значительно снижает качество судебной проверки обозначенных материалов.

Негативным последствием подобной ситуации становится повышение зависимости суда при принятии решения по уголовному делу от результатов закрепления доказательств следователем, дознавателем. Это снижает степень процессуальной самостоятельности суда при оценке электронных доказательств, может создавать риски одностороннего восприятия им доказательственной информации по уголовному делу, и как следствие принятие неправосудного решения, что противоречит предписаниям ст. ст. 88, 297 УПК РФ.

Наряду с изложенным отдельной составляющей рассматриваемой проблемы выступает недостаточный уровень технической подготовки участников уголовного процесса[312], включая судей. Электронные доказательства для исследования их судом могут быть представлены в виде: скриншота экрана,

---

[311] Развейкина Н. А., Шиханова Е. Г. Трансформации судопроизводства в России, спровоцированные пандемией // Вестник Омского университета. Серия «Право». 2021. Т. 18, № 4. С. 51-53.

[312] Малышева О. А. О новом векторе профессиональной подготовки следователя в условиях цифровой трансформации // Вестник Томского государственного университета. 2022 № 480. С. 262.

фотографии экрана, экспортированного файла переписки, отчета программ извлечения данных из мобильных устройств, файла с метаданными и др. В отсутствии соответствующих знаний о различии между этими видами электронных материалов затрудняется их правильную оценку. В частности, скриншот экрана и официальный отчет программы извлечения данных имеют различную доказательственную ценность по уголовному делу, однако при отсутствии должной технической подготовки субъектом уголовного процесса, равно и судьей, они могут восприниматься как равнозначные по юридической силе. Отмеченное влечет риск принятия судом неправосудного решения по уголовному делу, что более подробно было изложено выше в данной главе диссертации.

Решение проблемы недостаточной технической обеспеченности судов требует развития специализированной инфраструктуры судебной системы, оснащения судов защищенными рабочими станциями и программным обеспечением, позволяющим безопасно воспроизводить электронные носители и анализировать цифровые данные различных форматов, создания изолированной цифровой среды, внедрение единых технических стандартов оборудования в целях непосредственного исследования электронных материалов в судебном заседании, и повышения гарантий процессуальной самостоятельности суда в условиях интенсивной цифровизации.

Реализация указанного не достигнет положительного эффекта без повышения уровня технической подготовки участников уголовного процесса, более активного привлечения специалистов в области информационных технологий к исследованию электронных сведений для более полного определения технических характеристик электронной информации, всестороннего исследования электронных доказательств, вынесения по уголовному делу законного, обоснованного, мотивированного решения, основанного и на электронных доказательствах.

На основании изложенного можно сформулировать следующие выводы.

1. Действующая правовая регламентация процессуального порядка проверки доказательства (ст. 87 УПК РФ) распространяется на электронные доказательства, однако не учитывает их отличительные свойства, специальные критерии допустимости, что обуславливает проведение судом, как правило, формальных проверки и оценки таких доказательств. Отмеченное не согласуется с целью уголовно-процессуального доказывания.

2. Для современной практики проверки и оценки электронных доказательств по уголовному делу присущи ряд проблем: 1) ограничение действия принципа состязательности и равноправия сторон; 2) несоблюдение общего условия судебного разбирательства – непосредственность; 3) ненадлежащее распоряжение судом своих полномочий по исследованию электронных доказательств; 4) необоснованное сужение гарантий конституционных прав личности. Для преодоления указанного необходимо в уголовно-процессуальном законе:

– закрепить правила о непосредственном исследовании судом электронных носителей информации, обязательном использовании в судебном заседании процессуальных средств, способов, предусмотренных УПК РФ проверки достоверности электронных сведений;

– совершенствовать процессуальный порядок доступа суда к источникам электронной информации.

3. Недостаточный уровень материально-технического оснащения функционирования судов препятствует всестороннему, полному, объективному исследованию электронных уголовно-процессуальных доказательств (электронных данных) при рассмотрении уголовного дела по существу.

Заключение

1. Электронные доказательства обладают совокупностью специфических признаков, позволяющих рассматривать их как самостоятельное средство доказывания. Их особенности, связанные с цифровой формой существования, зависимостью от технической среды, риском изменения, утраты или искажения, обусловливают необходимость специального уголовно-процессуального регулирования. В связи с этим обоснована целесообразность законодательного закрепления понятия «электронное доказательство» и уточнения его места в системе доказательств, в том числе посредством внесения соответствующих изменений в ст. 74 УПК РФ.

2. Отсутствие в УПК РФ специальных критериев допустимости электронных доказательств осложняет разрешение вопросов, связанных с доступом к электронной информации, ее изъятием, копированием, сохранением и процессуальным закреплением. Это нередко влечет формальный подход к оценке допустимости электронных сведений. В диссертации обоснована необходимость нормативного закрепления специальных критериев допустимости электронных доказательств, включающих требования законности получения, аутентичности, целостности, прослеживаемости происхождения и последующей проверки.

3. Сравнительно-правовой анализ законодательства зарубежных государств позволил выявить, что доказательственное значение электронных данных определяется не их электронной формой, а соблюдением процессуальных условий их получения, фиксации, хранения и исследования. Целесообразно использование отдельных элементов зарубежного регулирования для совершенствования российского уголовно-процессуального законодательства, в том числе в части правовых средств установления происхождения электронных сведений, обеспечения их неизменности, определения допустимых пределов вмешательства в частную жизнь и укрепления процессуальных гарантий защиты.

4. Придание электронным сведениям доказательственного значения возможно лишь при соблюдении специальных правил их обнаружения, изъятия, сохранения, проверки и оценки. Особое значение имеют закрепление содержания электронных данных, их идентифицирующих признаков, источника происхождения, технических параметров и способа получения. Обоснована необходимость нормативного закрепления случаев обязательного участия специалиста и правил безотлагательного сохранения электронных сведений, имеющих значение для уголовного дела.

5. Исследование электронных доказательств не должно ограничиваться анализом их информационного содержания; необходима также проверка процессуальной формы их получения и закрепления, обеспечивающая возможность установить происхождение электронных сведений, а также подтвердить их сохранность и достоверность. Игнорирование различий между локально хранящимися и удаленно доступными сведениями, ошибки в интерпретации метаданных, недостоверное установление источника происхождения электронной информации, а также неполное исследование условий ее формирования и актуализации отрицательно влияют на результаты уголовно-процессуального доказывания и могут повлечь признание соответствующих сведений недопустимыми доказательствами.

6. Действующая регламентация проверки доказательств, закрепленная в ст. 87 УПК РФ, распространяется на электронные доказательства, однако фактически не учитывает их специфики. Это приводит к формальному характеру их исследования и оценки в суде, ограничению действия принципов состязательности, равноправия сторон и непосредственности судебного разбирательства, а также к недостаточной реализации судом своих полномочий по исследованию электронных носителей и электронных данных. Дополнительным фактором, затрудняющим всестороннее, полное и объективное исследование электронных доказательств, выступает недостаточный уровень материально-технического обеспечения судов.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

I. Международные правовые акты

1. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23.11.2001) // СПС «КонсультантПлюс» (дата обращения: 05.01.2026).

II. Правовые акты Российской Федерации

2. Конституция Российской Федерации, принята всенародным голосование 12 декабря 1993 года // СПС «КонсультантПлюс» (дата обращения: 03.11.2025).

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс» (дата обращения: 27.01.2026).

4. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

6. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

7. Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

8. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

9. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

10. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

11. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

III. Правовые акты зарубежных государств

12. Codice di procedura penale [Электронный ресурс] URL : https://www.studiocataldi.it/codiceproceduraрenale/codiceproceduraрenale.asp (дата обращения 21.01.2026).

13. Criminal Procedure Code of 27 November 2015 № 101/2015/QH13 [Электронный ресурс]. URL: https://www.wipo.int/wipolex/ru/ legislation/details/21477 (дата обращения: 21.01.2026).

14. Federal Rules of Evidence [Электронный ресурс]. URL: https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence (дата обращения: 21.01.2026).

IV. Судебная практика. Позиции высших судов Российской Федерации

15. Определение Конституционного Суда Российской Федерации от 04.02.1999 № 18-О «По жалобе граждан М. Б. Никольской и М. И. Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона «Об оперативно-розыскной деятельности» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

16. Определение Конституционного Суда Российской Федерации от 06.03.2003 № 104-О «Об отказе в принятии к рассмотрению запроса Бокситогорского городского суда Ленинградской области о проверке конституционности части первой статьи 86 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 16.04.2026).

17. Определение Конституционного Суда Российской Федерации от 02.10.2003 № 345-О «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» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

18. Определение Конституционного Суда Российской Федерации от 09.06.2005 № 248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

19. Определение Конституционного Суда Российской Федерации от 08.11.2005 № 439-О «По жалобе граждан С. В. Бородина, В. Н. Буробина, А. В. Быковского и других на нарушение их конституционных прав статьями 7, 29, 182 и 183 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

20. Определение Конституционного Суда Российской Федерации от 16.12.2008 № 1076-О-П «По жалобам граждан Арбузовой Елены Николаевны, Баланчуковой Александры Васильевны и других на нарушение их конституционных прав частями третьей и пятой статьи 165 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 04.02.2026).

21. Определение Конституционного Суда Российской Федерации от 28.06.2012 № 1253-О «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

22. Определение Конституционного Суда Российской Федерации от 26.01.2017 № 204-О «Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 УПК РФ» // СПС «КонсультантПлюс» (дата обращения: 05.05.2026).

23. Определение Конституционного Суда Российской Федерации от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 УПК РФ» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

24. Определение Конституционного Суда Российской Федерации от 17.07.2018 № 1955-О «Об отказе в принятии к рассмотрению жалобы гражданина Сидака Константина Петровича на нарушение его конституционных прав частью

шестой статьи 164 и статьей 177 УПК РФ» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

25. Определение Конституционного Суда Российской Федерации от 28.11.2019 № 3205-О «Об отказе в принятии к рассмотрению жалобы гражданина Габашвили Игоря Сергеевича на нарушение его конституционных прав частью первой статьи 176 и частью второй статьи 177 УПК РФ» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

26. Определение Конституционного Суда Российской Федерации от 24.06.2021 № 1364-О «Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 УПК РФ» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026).

27. Постановление Конституционного Суда Российской Федерации от 31.03.2011 года № 3-П «По делу о проверке конституционности части третьей статьи Уголовного кодекса Российской Федерации в связи с жалобами граждан С. В. Капорина, И. В. Коршуна и других» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026)

28. Постановление Конституционного Суда Российской Федерации от 16.06.2015 № 15-П «По делу о проверке конституционности положений статьи 139 Семейного кодекса Российской Федерации и статьи 47 Федерального закона «Об актах гражданского состояния» в связи с жалобой граждан Г. Ф. Грубич и Т. Г. Гущиной» // СПС «КонсультантПлюс» (дата обращения: 03.05.2026)

29. Постановление Конституционного Суда Российской Федерации от 17.12.2015 № 33-П «По делу о проверке конституционности пункта 7 части второй статьи 29, части четвертой статьи 165 и части первой статьи 182 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой граждан А. В. Баляна, М. С. Дзюбы и других» // СПС «КонсультантПлюс» (дата обращения: 05.05.2026)

30. Постановление Конституционного Суда Российской Федерации от 09.07.2020 № 34-П «По делу о проверке конституционности части второй статьи

313 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой администрации муниципального образования город Мурманск» // СПС «КонсультантПлюс» (дата обращения: 28.04.2026)

31. Постановление Пленума Верховного Суда Российской Федерации от 31.10.1995 № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

32. Постановление Пленума Верховного Суда Российской Федерации от 29.11.2016 № 55 «О судебном приговоре» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

33. Постановление Пленума Верховного Суда Российской Федерации от 01.06.2017 № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» // СПС «КонсультантПлюс» (дата обращения: 06.05.2026).

34. Постановление Пленума Верховного Суда Российской Федерации от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)» // СПС «КонсультантПлюс» (дата обращения: 17.04.2026).

35. Постановление Пленума Верховного Суда Российской Федерации от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

36. Постановление Пленума Верховного Суда Российской Федерации от 25.12.2018 №46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «КонсультантПлюс» (дата обращения: 04.02.2026).

37. Постановление Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

38. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 13.12.2018 по делу № 4-АПУ18-41 // ГАС «Правосудие» (дата обращения: 10.01.2026).

39. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 01.08.2019 по делу № 67-АПУ19-8 // ГАС «Правосудие» (дата обращения: 10.01.2026).

40. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 27.12.2017 по делу № 5-АПУ17-117 // СПС «КонсультантПлюс» (дата обращения: 05.05.2026)

41. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 13.12.2020 по делу № 223-АПУ19-4 // СПС «КонсультантПлюс» (дата обращения: 05.01.2026).

42. Кассационное определение Верховного Суда Российской Федерации от 30.09.2014 по делу № 2-18/08 // СПС «КонсультантПлюс» (дата обращения: 03.05.2026)

43. Кассационное определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 07.02.2023 № 5-КГ22-144-К2 // СПС «КонсультантПлюс» (дата обращения: 09.02.2026).

44. Кассационное определение Третьего кассационного суда общей юрисдикции от 01.01.2020 по делу № 77-870/2020 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

45. Кассационное определение Первого кассационного суда общей юрисдикции от 25.11.2020 по делу №77-2301/2020 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

46. Кассационное определение Восьмого кассационного суда общей юрисдикции от 23.12.2020 по делу № 77-3148/2020 // ГАС «Правосудие» (дата обращения: 15.01.2026).

47. Кассационное определение Первого кассационного суда общей юрисдикции от 09.01.2021 № 77-3490/2021 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

48. Кассационное определение Седьмого кассационного суда общей юрисдикции от 21.07.2021 № 77-2749/2021 // СПС «КонсультантПлюс» (дата обращения: 02.04.2025).

49. Кассационное определение Четвертого кассационного суда общей юрисдикции от 01.03.2022 № 77-852/2022 // СПС «КонсультантПлюс» (дата обращения: 12.05.2026).

50. Кассационное определение Второго кассационного суда общей юрисдикции от 14.11.2023 № 77-3590/2023 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

51. Кассационное постановление Первого кассационного суда общей юрисдикции от 16.01.2024 по делу № 77-204/2024 // СПС «КонсультантПлюс» (дата обращения: 05.01.2026).

52. Кассационное определение Первого кассационного суда общей юрисдикции от 31.01.2024 по делу № 77-454/2024 // СПС «КонсультантПлюс» (дата обращения: 12.05.2026).

53. Кассационное определение Второго кассационного суда общей юрисдикции от 21.01.2025 № 77-109/2025 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

54. Кассационное постановление Первого кассационного суда общей юрисдикции от 11.02.2025 № 77-469/2025 // СПС «КонсультантПлюс» (дата обращения: 12.05.2026).

55. Кассационное определение Первого кассационного суда общей юрисдикции от 27.02.2025 по делу № 77-629/2025 // СПС «КонсультантПлюс» (дата обращения: 10.02.2026).

56. Кассационное определение Первого кассационного суда общей юрисдикции от 20.05.2025 № 77-1553/2025// СПС «КонсультантПлюс» (дата обращения: 10.02.2026).

57. Кассационное определение Первого кассационного суда общей юрисдикции от 06.08.2025 № 77-2514/2025 // СПС «КонсультантПлюс» (дата обращения: 10.02.2026).

58. Кассационное постановление Шестого кассационного суда общей юрисдикции от 28 августа 2025 года № 77-2512/2025 // СПС «КонсультантПлюс» (дата обращения: 07.01.2026).

59. Кассационное постановление Третьего кассационного суда общей юрисдикции от 18.09.2025 по делу № 77-1758/2025 // СПС «КонсультантПлюс» (дата обращения: 07.01.2026).

60. Кассационное определение Первого кассационного суда общей юрисдикции от 07.10.2025 № 77-3195/2025 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

61. Кассационное постановление Девятого кассационного суда общей юрисдикции от 13.11.2025 № 77-1609/2025 // СПС «КонсультантПлюс» (дата обращения: 07.01.2026).

62. Кассационное определение Шестого кассационного суда общей юрисдикции от 27.11.2025 № 77-3328/2025; // СПС «КонсультантПлюс» (дата обращения: 07.01.2026).

63. Кассационное определение Первого кассационного суда общей юрисдикции от 17.12.2025 по делу № 77-3884/2025 // СПС «КонсультантПлюс» (дата обращения: 08.01.2026).

64. Кассационное определение Второго кассационного суда общей юрисдикции от 18.12.2025 № 77-3391/2025 // СПС «КонсультантПлюс» (дата обращения: 11.05.2026).

65. Апелляционное постановление судебной коллегии по уголовным делам Верховного Суда Республики Калмыкия от 29.01.2020 по делу № 22-23/2020 // ГАС «Правосудие» (дата обращения: 11.05.2026).

66. Апелляционное определение Московского городского суда от 12.03.2021 по делу № 10 1234/2021// «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 06.06.2026).

67. Апелляционное определение судебной коллегии по уголовным делам Свердловского областного суда от 25.11.2022 по делу №22-9081/2022 // ГАС «Правосудие» (дата обращения: 15.01.2026).

68. Апелляционное определение Московского городского суда от 03.06.2024 года по делу № 10-6860/2024 // «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 09.02.2026).

69. Апелляционное определение Московского городского суда от 28.07.2024 № 01-0011/2024 // «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 09.02.2026).

70. Апелляционное определение Московского городского суда от 13.11.2024 по делу № 10-22619/2024 // «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 09.02.2026).

71. Постановление Адлерского районного суда г. Сочи Краснодарского края от 19.06.2024 по делу № 3/1-115/2024 // ГАС «Правосудие» (дата обращения: 17.04.2025).

72. Приговор Нагатинского районного суда города Москвы от 13.08.2018 по делу № 1-419/2018 // Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 21.04.2026).

73. Приговор Ленинского районного суда г. Кирова от 14.02.2023 по делу № 1 45/2023 // ГАС «Правосудие» (дата обращения: 07.05.2026).

74. Приговор Хамовнического районного суда города Москвы от 11.12.2023 по делу № 1-85/2025 // Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

75. Приговор Наро-Фоминского городского суда Московской области от 31.10.2024 по делу № 1-358/2024. Доступ из ГАС «Правосудие» (дата обращения: 23.03.2025).

76. Приговор Наро-Фоминского городского суда Московской области от 15.01.2025 по делу № 1-13/2025. ГАС «Правосудие» (дата обращения: 05.05.2026).

77. Приговор Головинского районного суда города Москвы от 13.03.2025 по делу № 1-001/2025 // Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

78. Приговор Таганского районного суда города Москвы от 17.04.2025 по делу № 1-176/2025// Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

79. Приговор Перовского районного суда города Москвы от 13.11.2025 по делу № 1-1117/2025 // Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

80. Приговор Замоскворецкого районного суда города Москвы от 20.11.2025 по делу № 1-441/2025// «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 20.04.2026).

81. Приговор Останкинского районного суда города Москвы от 09.12.2025 года по делу № 1-764/2025 // Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

82. Приговор Кузьминского районного суда города Москвы от 29.01.2026 по делу № 1-0108/2026 // Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

83. Приговор Измайловского районного суда города Москвы от 19.03.2026 по делу № 1-158/2026 // «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 20.04.2026).

84. Приговор Останкинского районного суда города Москвы от 24.03.2026 по делу № 1-250/2026 // Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

85. Приговор Никулинского районного суда города Москвы от 29.05.2025 по делу № 1-0223/2025// Доступ «Официальный портал судов общей юрисдикции города Москвы» (дата обращения: 23.04.2026).

86. Материалы уголовного дела № 11901460030000704. СО по г. Подольск ГСУ СК России по Московской области.

87. Материалы уголовного дела № 12202280013040012. СУ СК России по Тверской области;

88. Материалы уголовного дела № 12302520006000129. СУ СК России по Омской области.

89. Материалы уголовного дела № 12302520006000081. СУ СК России по Омской области.

90. Материалы уголовного дела № 12401460026001945. ОД УМВД России по Одинцовскому городскому округу Московской области.

91. Материалы уголовного дела № 12401460024000312. СУ УМВД России по Наро-Фоминскому городскому округу.

92. Материалы уголовного дела № 12501009625000116. ЛУ МВД России в аэропорту Шереметьево.

93. Материалы уголовного дела 12501280014000105 МСО СУ СК РФ по Тверской области.

94. Материалы уголовного дела № 1250145045000025. СО ОМВД России по району Измайлово г. Москвы.

V. Книги. Монографии. Комментарии законодательства. Учебники и учебные пособия

95. Белкин, Р. С. Собирание, исследование и оценка доказательств. Сущность и методы / Р. С. Белкин. – М.: Наука, 1966. – 295 с.

96. Васюков, В. Ф., Расторопов, С. В., Флоря, Д. Ф. Получение и использование абонентской информации при расследовании преступлений / В. Ф. Васюков, С. В. Расторопов, Д. Ф. Флоря Орел, 2025. – 323 с.

97. Вехов, В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография / В. Б. Вехов. – Волгоград: Волгоградская академия МВД России, 2008. – 401 с.

98. Винберг, А. Й. Криминалистика: учебник для юридических вузов. Ч. 1 / под ред. А. И. Винберга. – М.: Государственное издательство юридическая литература, 1950. – 304 с.

99. Головко, Л. В. Курс уголовного процесса / под ред. Л. В. Головко. – М.: Статут, 2017. – 1280 с.

100. Гришин, Д. А. Информационные технологии уголовного судопроизводства / Д. А. Гришин. – Рязань: ИП Колупаева Е. В., 2024 – 168 с.

101. Зазулин, А. И. Использование цифровой информации в доказывании по уголовным делам / А. И. Зазулин. – М.: Юрлитинформ, 2019. – 312 с.

102. Зуев, С. В., Каменев, А. С. Собирание и проверка электронной доказательственной информации стороной защиты в уголовном судопроизводстве : монография / С. В. Зуев, А. С. Каменев. – М.: Юрлитинформ, 2024. – 158 с.

103. Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учебное пособие / Балашова А. А., Васюков В. Ф., Гаврилин В. Ф. и др. ; под ред. Ю. В. Гаврилина и А. В. Победкина. – М. : Академия управления МВД России, 2021. – 138 с.

104. Кипнис, Н. М. Допустимость доказательств в уголовном судопроизводстве / Н. М. Кипнис; отв. ред. П. А. Лупинская. – М.: Юрист, 1995. – 127 с.

105. Кудин, Ф. М., Костенко, Р. В. Допустимость доказательств в российском уголовном процессе : учебное пособие / Ф. М. Кудин, Р. В. Костенко. – Краснодар; Кубанский государственный аграрный университет. Юридический факультет, 2002 – 159 с.

106. Крупницкая, В. И. Теория доказательств и доказывание : курс лекций / В. И. Крупницкая – Новосибирск: СибАГС, 2011 – 160 с.

107. Курс советского уголовного процесса. Общая часть / под ред. А. Д. Бойкова, И. И. Карпеца. –М.: Юридическая литература, 1989. –638 с.

108. Лазарева, В. А. Доказывание в уголовном процессе: учебник для вузов / В.А. Лазарева. – М.: Юрайт, 2020. – 263 с.

109. Лупинская, П. А. Уголовно-процессуальное право: учебник / П. А. Лупинская. – М.: Норма, 2006. – 1008с.

110. Мещеряков, В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / А. В. Мещеряков. – Воронеж: ВГУ, 2002. – 407 с.

111. Основы теории электронных доказательств: монография / под ред. С. В. Зуева. – М.: Юрлитинформ, 2021. – 383 с.

112. Пастухов, П. С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества : монография / П. С. Пастухов ; под. ред. О. А. Зайцева. – М.: Юрлитинформ, 2015. – 347 с.

113. Петрухин, И. Л. Теоретические основы реформы уголовного процесса в России. Часть II / И. Л. Петрухин. – М.: Проспект, ТК Велби, 2005. – 192 с.

114. Россинская, Е. Р. Теория судебной экспертизы (Судебная экспертология) : учебник / Е. Р. Россинская, Е. И. Галяшина, А. М. Зинин ; под ред. Е. Р. Россинской. – М.: Норма : ИНФРА-М, 2026. – 368 с.

115. Смирнов А. В., Калиновский К. Б. Уголовный процесс : учебник для вузов / А. В.Смирнов, К. Б.Калиновский. – М. : Норма: ИНФРА-М, 2022 – 784 с.

116. Теория доказательств в советском уголовном процессе / под ред. Н. В. Жогина. – М.: Юридическая литература, 1973. – 736 с.

117. Уголовно-процессуальное право Российской Федерации : учебник / отв. ред. П. А. Лупинская. М.: Норма: ИНФРА-М, 2011 – 1087 с.

118. Шейфер, С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования: монография / С.А. Шейфер. – М.: Норма, 2008. – 238 с.

119. Шейфер, С.А. Собирание доказательств в советском уголовном процессе. Методологические и правовые проблемы / С.А. Шейфер. – Саратов: Изд-во Саратовского университета, 1986. – 169 с.

120. Электронные доказательства в уголовном судопроизводстве: учеб. пособие для вузов / под ред. С.В. Зуев. – М.: Юрайт, 2025. – 193 с.

VI. Научные статьи

121. Архипова, Н. А. К вопросу об использовании возможностей средств мобильной связи в раскрытии и расследовании преступлений / Н. А. Архипова // Сборник материалов криминалистических чтений. Барнаул, 2014. – № 10. – С. 16-17.

122. Багмет, А. М., Скобелин, С. Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие / А. М. Багмет, С. Ю. Скобелин // Право и кибербезопасность. – 2013. – № 2. – С. 22-27.

123. Багмет, А. М., Скобелин, С. Ю. Пределы ограничения конституционных прав граждан в ходе осмотра сотовых телефонов участников уголовного судопроизводства / А. М. Багмет, С. Ю. Скобелин // Уголовное право. – 2017. – № 6. – С. 103-108.

124. Балашова, А. А. К вопросу о понятии «Электронное доказательство» / А. А. Балашова // Закон и право. – 2018. – №6. – С.120–122.

125. Баранова, М. А., Мишкина, М. Д. Проблемы аутентификации цифровых доказательств: исследование методов проверки подлинности электронных писем в суде // Государственно-правовые явления: история и современность (ко Дню Российской науки) : сборник научных статей Всероссийской научно-практической конференции. – Саратов, 2025. – С. 18-22.

126. Бачило, А. Н. Достоверность электронных доказательств: проблемы верификации / А. Н. Бачило // Вестник цифрового права. – 2019. – № 3 (12). – С. 45-52.

127. Белкин, А. Р. Еще раз о доказательствах, об источниках доказательств и о том, как отличить одно от другого / А. Р. Белкин // Мировой судья. – 2012. – № 1. – С. 10-15.

128. Бикмиев, Р. Г., Бурганов, Р. С. Собирание электронных доказательств в уголовном судопроизводстве / Р. Г. Бикмиев, Р. С. Бурганов // Информационное право. – 2015. – № 3. – С. 17-21.

129. Боруленков Ю. П. Допустимость доказательств: время перемен? / Ю. П. Боруленков // Уголовное судопроизводство. – 2013. – № 3. – С. 16-20.

130. Будников В. Л. Субъекты обязанности доказывания в уголовном судопроизводстве / В. Л. Будников // Российская юстиция. – 2008. – № 5. – С. 27-30.

131. Бычков В. В. Соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при проверке сообщений о преступлениях и в ходе их расследования / Бычков В. В. // Российский следователь. – 2013. – № 24. – С. 11-15.

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

133. Волынский, А. Ф. Научно-техническое обеспечение судопроизводства: привычные проблемы и программно-целевой подход к их решению / А. Ф. Волынский // Известия Тульского государственного университета. Экономические и юридические науки. – 2023. – № 2. – С. 3-12.

134. Воронин, М. И. Электронные доказательства в УПК: быть или не быть? / М. И. Воронин // Lex russica. – 2019. – № 7 (152). – С. 74-84.

135. Воскобитова, Л. А. Понятие доказательства и использование «цифровой» информации в доказывании по уголовному делу / Л. А. Воскобитова // Высокотехнологичное право: современные вызовы: материалы IV Международной межвузовской научно-практической конференции. – Красноярск, 2023. – С. 57-64.

136. Гаврилин, Ю. В. Электронные носители информации в уголовном судопроизводстве / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2017. – №4 (44). – С.45-50.

137. Газизов, В. А., Подволоцкий, И. Н. Меры обеспечения цифровой криминалистики / В. А. Газизов, И. Н. Подволоцкий // Энциклопедия Судебной Экспертизы. – № 1 (24) – 2020. – С. 21-28.

138. Галяшина, Е. И. Современные проблемы использования цифровых доказательств в уголовном процессе / Е. И. Галяшина // Вестник Московского университета МВД России. – 2022. – № 4. – С. 67–73.

139. Галяшина, Е. И., Шамаев, Г. П. Обеспечение достоверности материалов оперативно-розыскных мероприятий как доказательств в уголовном судопроизводстве / Е. И. Галяшина, Г. П. Шамаев // Криминалистика и судебная экспертиза. – СПб., 2012. – С. 492-499.

140. Ганага, В. С. К вопросу о допустимости цифровых доказательств в уголовном процессе / В. С. Ганага // Санкт-Петербургские встречи молодых ученых: материалы II Всероссийского конгресса. – Санкт-Петербург, 2024. – С. 522-526.

141. Гасанов, И. Т. К вопросу о получении судебного разрешения на осмотр сотовых телефонов участников уголовного процесса на досудебных стадиях / И. Т. Гасанов // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий: сборник научных статей /отв. ред. С.И. Давыдов, В.В. Поляков. – Барнаул. – 2018. Вып. XV. – С. 72-79.

142. Гмурко, В. П. Парадоксы доказательственного права / В. П. Гмурко // Библиотека криминалиста. – 2014. – № 2. – С. 9-17.

143. Головко, Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? / Л. В. Головко // Вестник экономической безопасности. – 2019. – С. 15-25.

144. Грачев, С. А. Тайна телефонных переговоров в правовых позициях высших судебных инстанций России: коллизия толкований / С. А. Грачев // Законы России: опыт, анализ, практика. – 2020. – № 2. – С. 81-85.

145. Гурдин, С. В. Собирание и представление доказательств защитником – реальность или процессуальная иллюзия? / С. В. Гурдин // Криминологический журнал. 2020. – № 4. – С. 50-55.

146. Даниленко, И. А., Васильев, Н. В. Соблюдение конституционных прав личности на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, почтовых, телеграфных и иных сообщений при осмотре мобильного устройства (российский и зарубежный опыт) / И. А. Даниленко, Н. В. Васильев // Вестник Университета имени О. Е. Кутафина (МГЮА). 2020. – № 10. – С. 150-157.

147. Демидов, Н. Н., Фам, Н. Х. Проблемы, связанные со сбором и использованием электронных доказательств в уголовном деле во Вьетнаме / Н. Н. Демидов, Н. Х. Фам // Закон и право. – 2021. – № 1. – С. 87-90.

148. Жамкова О. Е. Юридическая значимость сведений, полученных защитником по уголовному делу / О. Е. Жамкова // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : сборник научных статей. – Орел, 2024. – С. 88-90.

149. Желева, О.В. К вопросу о понятии электронных доказательств и критериях допустимости их использования / О.В. Желева // Уголовная юстиция. – 2021. – №17. – С. 44–49.

150. Журкина, О. В. Электронные доказательства: понятие и признаки / О.В. Журкина // Российская юстиция. – 2020. – № 9. – С. 44-46.

151. Зуев, С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) / С. В. Зуев // Пермский юридический альманах. – 2019. – № 2. – С. 618-629.

152. Зуев, С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение / С. В. Зуев // Правопорядок: история, теория, практика. – 2020. – № 3 (26). – С. 46-51.

153. Зуев, С. В. Электронная информация и ее носители в уголовно-процессуальном доказывании: развитие правового регулирования / С. В. Зуев // Вестник ЮУрГУ. – 2017. – Т. 17, № 1. – С. 31-35.

154. Иванова, Е. В. Скриншот – цифровая возможность в процессе доказывания: проблемные аспекты / Е. В. Иванова // Право и государство: теория и практика. – 2019. – № 12(180). – С. 180-182.

155. Каламов, Ж. С. Актуальные проблемы действия электронных доказательств на судебной стадии уголовного судопроизводства в Российской Федерации и странах с континентальной системой права / Ж. С. Каламов // Аграрное и земельное право. – 2023. – № 3 (219). – С. 214-217.

156. Каламов, Ж. С. Правовое регулирование электронных доказательств в странах с континентальной системой права: опыт Франции и Германии / Ж. С. Каламов // Евразийский юридический журнал. – 2021. – № 4 (155). – С. 318-320

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

158. Калитин, С. В. Доказательства электронные и цифровые / С. В. Калитин // Научно-методический электронный журнал «Концепт». – 2014. – Т. 20. – С. 3586-3590.

159. Карташов, И. И. Проблемы формирования доказательств в уголовном судопроизводстве на основе цифровой информации / И. И. Карташов // Юридическая наука. – 2018. – № 3. – С. 99-103.

160. Карякин, Е. А., Миронов, В. К вопросу о взаимосвязи достоверности с иными свойствами доказательств / Е. А. Карякин, В. К Миронов // Уголовное право. – 2004. – № 3. – С. 85-86.

161. Квасница, С. Е., Бирюков, С. Ю. Электронные доказательства: проблемы допустимости в уголовном судопроизводстве / С. Е. Квасница, С. Ю. Бирюков // Вестник Волгоградской академии МВД России. – 2024. – № 2 (69). – С. 101-107.

162. Козловский, П. В., Седельников, П. В. Участие специалиста в изъятии электронных носителей / П.В. Козловский, П. В. Седельников // Научный вестник Омской академии МВД России. – 2014. – № 1 (52). – С. 17-19.

163. Колдин, В. Я. Электронная информация в праве / В. Я. Колдин // Вестник Московского университета. Серия 11: Право. – 2016. – № 2. – С. 96-110.

164. Количенко, А. А. Отдельные аспекты проверки электронных доказательств в уголовном процессе / А. А. Количенко // Проблемы юридической науки в исследованиях адъюнктов и соискателей. – М., 2022. Вып. 28. – С. 107-116.

165. Количенко, А. А. О специфике проверки электронных доказательств в уголовном процессе / А. А. Количенко // Альманах молодых ученых. – 2022. – № 2. – С. 108-114.

166. Костенко, Р. В. Процессуальные действия как способ проверки доказательств в уголовном судопроизводстве / Р. В. Костенко // Юридический вестник Кубанского государственного университета. – 2020. – № 3. – С. 46-50.

167. Куценко, Т. М., Здольник, В. В. Электронные документы как современный вид доказательств по делу об административном правонарушении / Т. М. Куценко, В. В. Здольник // Вестник Московского университета МВД России. – 2014. – № 6. – С. 195-202.

168. Литвин, И. И. Некоторые особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий / И.И. Литвин // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. – 2020. – № 1(53). – С.8-13.

169. Макарова, Е. В. Роль электронных доказательств в уголовном процессе США и Российской Федерации / Е. В. Макарова // Инновационный потенциал развития науки в современном мире: технологии, инновации, достижения: сборник научных статей по материалам XIII Международной научно-практической конференции. – Уфа, 2023. – С. 62-66.

170. Маламагамедова, А. Р. «Электронные доказательства» в уголовном процессе /А. Р. Маламагамедова // Уголовная политика России на современном этапе: состояние, тенденции, перспективы. – М., 2024. – С. 287-291.

171. Малов А. А. Получение электронных доказательств от иностранных юрисдикций (на примере США) / А. А. Малов // Законность. – 2018. – № 9 (1007). – С. 57-60.

172. Малышева, О. А. Особенности доказывания, осуществляемого следователем, в условиях цифровизации уголовного судопроизводства / О. А. Малышева // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2020. – № 10 (74). – С. 82-88.

173. Малышева, О. А. Процессуальная форма участия защитника в доказывании в досудебном производстве требует оптимизации / О. А. Малышева // Актуальные проблемы российского права. – 2023. – Т. 18. № 5 (150). – С. 123-130.

174. Малышева, О. А. О новом векторе профессиональной подготовки следователя в условиях цифровой трансформации / О. А. Малышева // Вестник Томского государственного университета. – 2022. – № 480. – С. 262-268.

175. Марковичева Е. В., Рябинина Т. К. Гласность судебного разбирательства по уголовным делам: баланс публичных и частных интересов / Е. В. Марковичева, Т. К. Рябинина // Правосудие. – 2024. – Т. 6. № 4. – С. 132-150.

176. Можаева, И. П., Шульгин, Е. П. О понимании доказательств в правоохранительной деятельности в эпоху цифровых преобразований / И. П. Можаева, Е. П. Шульгин // Юристъ-Правоведъ. – 2022. – № 4 (103). – С. 162-167.

177. Никурадзе, Н. О. К вопросу об оценке «электронных доказательств» в уголовном судопроизводстве в контексте российского и зарубежного опыта / Н. О. Никурадзе // Вестник Томского государственного университета. – 2024. – № 508. – С. 258–269.

178. Нгуен, Т. Н. Ч. Доказательства, полученные из электронных источников в уголовном судопроизводстве Вьетнама / Т. Н. Ч. Нгуен // Universum: экономика и юриспруденция. – 2024. – № 9 (119). – С. 63-65.

179. Нгуен, Т. Б., Тью, В. Х., Нгуен, В. Ч. К вопросу о сборе и анализе электронных доказательств из памяти компьютера при расследовании киберпреступлений в Социалистической Республике Вьетнам / Т. Б. Нгуен,

В. Х. Тью, В. Ч. Нгуен // Universum: экономика и юриспруденция. – 2024. – № 4-1 (114). – С. 50-54.

180. Облаков А. А. Цифровые доказательства в уголовном процессе: проблемы сбора и оценки / А. А. Облаков // Закон и власть. – 2024. – № 5. – С. 156-158.

181. Оконенко, Р. И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р. И. Оконенко // Актуальные проблемы российского права. – 2015. – № 3 (52). – С.120-124.

182. Олиндер, Н. В. К вопросу о доказательствах, содержащих цифровую информацию / Н. В. Олиндер // Юридический вестник Самарского университета. – 2017. – № 3. – С. 107-110.

183. Отченаш, А. Ю. К вопросу о критериях допустимости «электронных доказательств» в уголовном судопроизводстве / А. Ю. Отченаш // Вестник Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации. – 2022. – №3 (95). – С.80-85.

184. Пастухов, П. С. «Электронные доказательства» в нормативной системе уголовно-процессуальных доказательств / П. С. Пастухов // Пермский юридический альманах. – 2019. – № 2. – С. 695-707.

185. Пастухов, П. С. О необходимости замены в уголовном судопроизводстве письменного протокола электронным документом / П. С. Пастухов // Научный вестник Омской академии МВД России. – 2015. – № 3. – С. 21-24.

186. Пастухов, П. С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств / П. С. Пастухов // Седьмой Пермский конгресс ученых-юристов: сборник научных статей. – Пермь, 2017. – С. 558-566.

187. Перцев, М. С. Безопасность данных и цифровые следы: обеспечение целостности электронных доказательств в уголовном процессе / М. С. Перцев // Бизнес. Образование. Право. – 2025. – № 2 (71). – С. 213-218.

188. Победкин, А. В. Публичность уголовного судопроизводства и ее отражение в доказательственном праве / А. В. Победкин // Труды Академии управления МВД России. – 2018. – № 4 (48). – С. 135-141.

189. Развейкина, Н. А., Шиханова, Е. Г. Трансформации судопроизводства в России, спровоцированные пандемией / Н. А. Развейкина, Е. Г. Шиханова // Вестник Омского университета. Серия «Право». – 2021. – Т. 18. – № 4. – С. 51-53.

190. Рамалданов, Х. Х. Проблемы использования и хранения цифровых доказательств в доказывании в уголовном процессе / Х. Х. Рамалданов // Вестник Казанского юридического института МВД России. – 2023. – Т. 14. № 2 (52). – С. 107-112.

191. Рогава, И. Г., Датумян, С. С., Куренная А. А. Цифровые доказательства в российском уголовном процессе: история, проблемы и перспективы развития / И. Г. Рогава, С. С. Датумян, А. А. Куренная // Проблемы экономики и юридической практики. – 2021. – Т. 17. – № 1. – С. 245-249.

192. Россинская, Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е. Р. Россинская // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2019. – № 5 (57). – С. 35-41.

193. Россинский, С. Б. Собирание доказательств как «первый» этап доказывания по уголовному делу / С. Б. Россинский // Юридический вестник Самарского университета. – 2020. – Т. 6. № 3. – С. 91-103.

194. Рудин, А. В. Основные теоретические проблемы проверки доказательств на стадии досудебного производства в уголовном процессе / А. В. Рудин // Закон и право. – 2018. – № 3. – С. 111-114.

195. Русман, Г. С., Морозова, Ю. А. Применение цифровых технологий в уголовном судопроизводстве: на примере судебной экспертизы / Г. С. Русман, Ю. А. Морозова // ЕВРАЗИЯ-2022: социально-гуманитарное пространство в эпоху глобализации и цифровизации. Т. I. Цифровое общество. Гуманизация. Глобализация. Молодежная политика : материалы Международного научного

культурно-образовательного форума – Челябинск : Издательский центр ЮУрГУ, 2022. – С. 200-203.

196. Русман, Г. С., Смолин, М. С. Правомочия стороны защиты в цифровом уголовном судопроизводстве / Г. С. Русман, М. С. Смолин // Правопорядок: история, теория, практика. – 2026. – № 1 (48). – С. 166-172.

197. Русман, Г. С., Сурменева, С. В. Цифровые инструменты в примирительных процедурах уголовного судопроизводства: современное состояние и перспективы / Г. С. Русман, С. В. Сурменева // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития. – СПб., 2023. – С. 256-262.

198. Русман, Г. С., Тетюев, С. В. Отзыв ведущей организации о кандидатской диссертации Х. Х. Рамалданова «Процесс доказывания по уголовным делам в условиях тотальной цифровизации общественных отношений» / Г. С. Русман, С. В. Тетюев // Вестник Южно-Уральского государственного университета. Серия: Право. – 2025. – Т. 25. – № 1. – С. 115-122.

199. Рябинина, Т. К. И вновь к вопросу об активной роли суда в уголовном судопроизводстве / Т. К. Рябинина // Тенденции уголовной политики России на современном этапе развития общества. Ижевск, 2024. С. 59-67.

200. Рябинина, Т. К. Роль суда в обеспечении баланса частных и публичных интересов в уголовном судопроизводстве // Российское правосудие. 2022. № 2. С. 78-88.

201. Рябинина, Т. К., Ряполова, Я. П., Чистилина, Д. О. Актуальные проблемы выявления и расследования дистанционных хищений с банковского счета / Т. К. Рябинина, Д. О. Чистилина, Я. П. Ряполова // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. – 2023. – № 4. – С. 31-38.

202. Рябинина, Т. К., Ряполова, Я. П. Перспективные направления использования искусственного интеллекта в доказывании по уголовным делам / Т. К. Рябинина, Д. О. Чистилина // Проблемы правоохранительной деятельности. – 2025. – № 3. – С. 23-29.

203. Рябинина, Т. К., Ряполова, Я. П., Чистилина, Д. О. Цифровая трансформация уголовно-процессуального доказывания: преимущества и риски / Т. К. Рябинина, Д. О. Чистилина, Я. П. Ряполова // Вестник Томского государственного университета. – 2025. – № 516. – С. 225-232.

204. Рябинина, Т. К., Ряполова, Я. П. Использование цифровых технологий в ходе судебного разбирательства по уголовному делу: проблемы и перспективы / Т. К. Рябинина, Д. О. Чистилина // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2025. – № 3 (104). – С. 301-306.

205. Ряховская, Я. О. Электронно-информационные технологии в уголовном процессе США // Инновации в информационных технологиях, машиностроении и автотранспорте: сборник материалов V Международной научно-практической конференции / Я. О. Ряховская. ред. кол.: Д. М. Дубинкин (отв. ред.) и др. – Кемерово, 2021. – С. 150-153.

206. Сергеев, М. С. Электронные доказательства в уголовном судопроизводстве: опыт США / М. С. Сергеев // Вестник экономики, права и социологии. – 2016. – № 2. – С. 210-213

207. Смирнов, К. А. Об «электронных» доказательствах по уголовно-процессуальному законодательству зарубежных государств / К. А. Смирнов // Правовая система и вызовы современности: материалы XX Международной научно-практической конференции студентов, аспирантов и молодых ученых. – Уфа, 2023. – С. 934-943.

208. Соколов А. Б., Третьякова Е. И. Осмотр мобильного телефона: неразрешенные вопросы правоприменения / А. Б. Соколов, Е. И. Третьякова // Криминалистика: вчера, сегодня, завтра. – 2023. – Т. 26. № 2. – С. 223-224.

209. Степаненко, Д. А. Технология собирания электронно-цифровых доказательств: проблемы и рекомендации / Д. А. Степаненко // ГлаголЪ правосудия. – 2024. – № 1 (35). – С. 24-29.

210. Сущенко, С. А. Электронные доказательства в уголовном процессе США / С. А. Сущенко // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2024. – № 1 (98). – С. 230-233.

211. Тимофеев, С. В., Кочесоков, Р. Х. Перспективы совершенствования российского законодательства в области использования цифровых следов преступления / С. В. Тимофеев, Р. Х. Кочесоков // Вестник Восточно-Сибирского института МВД России. – 2024. – № 4 (111). – С. 270-276.

212. Титова, К. А., Литвинова, И. В. К вопросу о возможности применения существующих критериев допустимости доказательств к электронным доказательствам в российском уголовном процессе / К. А. Титова, И. В. Литвинова // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2022. – № 2. – С. 144-152.

213. Токарева, Е. В., Хоршева, В. С. Осмотр электронных сообщений: правовая регламентация и особенности производства / Е. В. Токарева, В. С. Хоршева // Уголовное судопроизводство России: проблемы и перспективы развития: материалы всероссийской науч.-практ. конф. Санкт-Петербург, ноября 2019 года. – СПб., – 2019. – С. 348-353.

214. Туршин, А. И. Электронные доказательства в уголовном процессе: опыт зарубежных стран и российские перспективы /А. И. Туршин // Юридические исследования. 2025. – № 9. – С. 9-18.

215. Удовиченко, В. С., Сорокина, С. А. Особенности изъятия информации с электронных носителей в досудебном производстве / В. С. Удовиченко, С. А. Сорокина // Алтайский юридический вестник. – 2021. – № 2 (34). – С. 133-138.

216. Фам, Н. Х. Допустимость в качестве доказательства и доказательная сила электронных данных в уголовном судопроизводстве Социалистической Республики Вьетнам / Н. Х. Фам // Актуальные проблемы организации правоохранительной и правозащитной деятельности: материалы международной научно-практической конференции / отв. ред. В. Н. Яшин. – Тула, 2022. – С. 189-193.

217. Фам, Н. Х. К вопросу применения электронных данных в уголовном судопроизводстве Вьетнама / Н. Х. Фам // Вопросы российской юстиции. – 2023. – № 27. – С. 607-611.

218. Фам, Н. Х. Некоторые трудности при сборе электронных доказательств в Республике Вьетнам / Н. Х. Фам // Материалы Весенней Международной научно-практической сессии института права: Международного круглого стола «Умные технологии правового обеспечения конкурентоспособной предпринимательской среды», Международной научно-практической конференции «Судопроизводство в Российской Федерации и за рубежом: вопросы истории и проблемы современности». – 2021. – С. 199-203.

219. Фам, Н. Х., Во С. К. Некоторые вопросы о собирании и использовании электронных данных в уголовных делах / Н. Х. Фам, С. К. Во // Вопросы российской юстиции. – 2021. – № 16. – С. 427-428.

220. Фам, Н. Х., Во С. К., Ха К. А. Электронные доказательства и принципы собирания в уголовном судопроизводстве Вьетнама / Н. Х. Фам, С. К. Во, К. А. Ха // Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений: сборник научных статей по итогам работы двенадцатого круглого стола со Всероссийским и международным участием. – Шахты, 2020. – С. 151-155.

221. Федулова, А. Е. Электронные доказательства в уголовном процессе: процессуальная форма и порядок получения / А. Е. Федулова // Закон и право. – 2023. – № 5. – С. 45-49.

222. Федулова, А. Е. Электронные носители информации в уголовном судопроизводстве / А. Е. Федулова // Юридическая наука и правоохранительная практика. 2022. – № 2. – С. 90-100.

223. Фильченко А. П., Жандров В. Ю. Соблюдение законности при получении информации с электронных мобильных устройств, принадлежащих задержанным / А. П. Фильченко, В. Ю. Жандров // Российское правосудие. – 2018. – № 3 (143). – С. 85-91.

224. Харисова З. И. Проблемы и пути совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации /Харисова З. И. // Вестник Уфимского юридического института МВД России. – 2025. – № 2 (108). – С. 122-128.

225. Химичева, О. В. Следственные действия: о цифровой трансформации их производства / О. В. Химичева // Криминологический журнал. – 2023. – № 2. – С. 172-178.

226. Химичева, О. В. Развитие уголовно-процессуального доказывания в условиях цифровой трансформации / О. В. Химичева // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности: сб. науч. ст. по материалам международной научно-практической конференции. – М., 2023. – С. 187-188.

227. Химичева, О. В., Панфилов, П. О. Изменение уголовно-процессуальной формы в условиях цифровизации: новые риски и возможности / О. В. Химичева, П. О. Панфилов // Вестник Московского университета МВД России. – 2024. – № 1. – С. 161-166.

228. Чан, К. Х. Электронные доказательства при расследовании преступлений, посягающих на национальную безопасность во Вьетнаме / К. Х. Чан // Universum: экономика и юриспруденция. – 2026. – № 2-2 (136). – С. 37-41.

229. Чеботарева И. Н., Лунева К. А., Рейц А. Н. Актуальные вопросы использования аудиозаписи в качестве доказательства в уголовном процессе / И. Н. Чеботарева, К. А. Лунева, А. Н. Рейц // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. – 2025. – № 3. – С. 72-78.

230. Черданцев, А. Ю. Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе / А. Ю. Черданцев // Юридическая наука и практика. – 2019. – № 4. – С. 55-60.

231. Черецких, А. В. Цифровые (электронные) доказательства в уголовном судопроизводстве / А. В. Черецких // Правопорядок: история, теория, практика. – 2023. – № 4 (39). – С. 110–117.

232. Черкасов, В. С. Почему в российском уголовном процессе необходимо совершенствовать гарантии защиты тайны «электронных коммуникаций»? / В. С. Черкасов // Вестник Московского университета МВД России. – 2021. – № 4. – С. 130-136

233. Черкасов, В. С. Тайна «электронных коммуникаций» в уголовном процессе России, США, Китая и Германии / В. С. Черкасов // Проблемы правовой и технической защиты информации. – 2020. – № 8. – С. 114-118.

234. Чернышов, В. Н., Лоскутова, Е. С. Проблемы собирания и использования цифровых доказательств / В. Н. Чернышов, Е. С. Лоскутова // Социально-экономические явления и процессы. – 2017. – Т. 12. № 5. – С. 199-203.

235. Чич, Ю. А., Романов, А. В. Процессуальные особенности собирания электронных доказательств в социальных сетях / Ю. А. Чич, А. В. Романов // Вестник экономики и права. – 2026. – № 113. – С. 259-266

236. Шампаров, А. В. Механизм следообразования информации о соединениях между абонентами и (или) абонентскими устройствами / А. В. Шампаров // Вестник Удмуртского университета. Серия Экономика и право. 2014. № 4. С. 203-208.

237. Шаталов, А. С. Роль, сущность и значение цифровых (электронных) доказательств в уголовном судопроизводстве / А. С. Шаталов // Вестник Томского государственного университета. – 2024. – № 500. – С. 231-237.

238. Шильникова А. А. Электронные доказательства в уголовном процессе: понятие и критерии допустимости их использования / А. А. Шильникова // Проблемы права: теория и практика. – 2022. – № 60. – С. 298-303.

239. Юрченко И. А. Нарушение телекоммуникационной тайны в контексте российского уголовного права: текущие проблемы и перспективы их преодоления / И. А. Юрченко // Lex russica. – 2023. – Т. 76. № 9. – С. 44-52.

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

241. Янин, М. Г. Проблемы сбора, проверки и оценки электронных доказательств в уголовном судопроизводстве / М. Г. Янин, К. М. Кочедыкова // Управление в современных системах. – 2019. – № 2 (22). – С. 28-31.

VII. Диссертации. Авторефераты диссертаций

242. Адильшаев Э. А. Судебное санкционирование в уголовном процессе России : автореф. дис. … канд. юрид. наук: 12.00.09 / Адильшаев Эмиль Айдерович. – Ижевск, 2011 – 29 с.

243. Балакшин, В. С. Доказательства в теории и практике уголовно-процессуального доказывания (важнейшие проблемы в свете УПК Российской Федерации) : дис. … д-ра юрид. наук: 12.00.09 / Виктор Степанович Балакшин. – Екатеринбург, 2005. – 533 с.

244. Балашова, А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. … канд. юрид. наук: 12.00.09 / Анна Александровна Балашова. – М., 2020. – 210 с.

245. Бестаев, А. О. Способы собирания доказательств в уголовном процессе России : дис. … канд. юрид. наук: 12.00.09 / Алан Омарович Бестаев – Нижний Новгород, 2007. – 229 с.

246. Бирмамитова, С. А. Доказывание на досудебных стадиях уголовного процесса по делам о преступлениях, совершенных осужденными в исправительных колониях : дис. … канд. юрид. наук: 12.00.09 / Светлана Альбертовна Бирмамитова. – М., 2007. – 201 с.

247. Васин, В. В. Уголовно-процессуальное познание судом первой инстанции обстоятельств уголовного дела : автореф. дис. … канд. юрид. наук: 12.00.09 / Вячеслав Викторович Васин. – Томск, 2006. – 34 с.

248. Горелов, М. В. Электронные доказательства в гражданском судопроизводстве России: вопросы теории и практики : автореф. дис. … канд. юрид. наук: 12.00.15 / Максим Владимирович Горелов. – Екатеринбург, 2005. – 21 с.

249. Егорова, Т. З. Средства доказывания и их оценка в судебных стадиях российского уголовного процесса : дис. … канд. юрид. наук: 12.00.09 / Татьяна Зинуровна Егорова. – Ижевск, 2003. – 162 с.

250. Ерпылев, И. В. Реализация института допустимости доказательств в уголовном процессе и правоохранительной деятельности России и зарубежных государств (сравнительно-правовой анализ): автореф. дис. ... канд. юрид. наук: 12.00.09, 12.00.11 / Илья Владимирович Ерпылев. – М., 2016. – 30 с.

251. Зазулин, А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. ... канд. юрид. наук : 12.00.09 / Анатолий Игоревич Зазулин. – Екатеринбург, 2018. – 251 с.

252. Зигура, Н. А. Компьютерная информация как вид доказательств в уголовном процессе: дис. ... канд. юрид. наук: 12.00.09 / Надежда Анатольевна Зигура. – Челябинск, 2010. – 234 с.

253. Карпенко, В. М. Оценка доказательств следователем и дознавателем : дис. … канд. юрид. наук: 12.00.09 / Валерия Михайловна Карпенко. М., 2007. – 210 с.

254. Количенко А. А. Проблемы проверки и оценки электронных доказательств в современном уголовном процессе: дис. ... канд. юрид. наук: 5.1.4 / Артем Андреевич Количенко. – Нижний Новгород, 2023. – 224 с.

255. Костенко, Р. В. Доказательства в уголовном процессе: концептуальные подходы и перспективы правового регулирования: дис. ... док-ра. юрид. наук: 12.00.09 / Роман Валерьевич Костенко. – М., 2006. – 421 с.

256. Кузнецов, Н. П. Доказывание и его особенности на стадиях уголовного процесса России : дис. … д-ра юрид. наук: 12.00.09 / Николай Пантелеймонович Кузнецов. Воронеж, 1998. – 444 с.

257. Ларинков, А. А. Теоретические и правоприменительные проблемы доказывания на стадии судебного разбирательства : автореф. дис. … канд. юрид. наук: 12.00.09 / Анатолий Александрович Ларинков. – СПб., 2006. – 25 с.

258. Муратова, Н. Г. Система судебного контроля в уголовном судопроизводстве: вопросы теории, законодательного регулирования и практики : автореф. дис. … д-ра юрид. наук : 12.00.09 / Надежда Георгиевна Муратова. – Екатеринбург, 2004. – 46 с.

259. Набатов, М. Б. Реализация права на защиту в уголовном процессе в условиях применения цифровых технологий : автореф. дис. … канд. юрид. наук: 5.1.4 / Михаил Борисович Набатов. – М., 2024. – 28 с.

260. Оконенко, Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства США и РФ: дис. … канд. юрид. наук: 12.00.09 / Роман Иванович Оконенко. – М., 2016. – 158 с.

261. Пастухов, П. С. Модернизация уголовно-процессуального доказывания в условиях информационного: дис. ... канд. юрид. наук: 12.00.09 / Павел Сысоевич Пастухов. – М., 2015. – 454 с.

262. Пастухов, П. С. Модернизация уголовно-процессуального доказывания в условиях информационного: автореф. дис. ... канд. юрид. наук: 12.00.09 / Павел Сысоевич Пастухов. – М., 2015. – 64 с.

263. Пиюк, А. В. Роль суда в собирании доказательств по уголовному делу на стадии предварительного расследования и при рассмотрении дела в суде первой инстанции : автореф. дис. … канд. юрид. наук: 12.00.09 / Алексей Валерьевич Пиюк. – Томск, 2004. – 29 с.

264. Плашевская, А. А. Собирание судом доказательств при рассмотрении дела по первой инстанции в уголовном процессе России : автореф. дис. … канд. юрид. наук: 12.00.09 / Анастасия Анатольевна Плашевская. – Томск, 2006. – 27 с.

265. Рамалданов Х. Х. Процесс доказывания по уголовным делам в условиях тотальной цифровизации общественных отношений : дис. … канд. юрид. наук: 5.1.4 / Рамалданов Ханбулат Хизриевич. – М., 2024. – 244 с.

266. Ремизова М. С. Теоретические и правовые основы формирования допустимых доказательств в условиях состязательного уголовного процесса : дис. … канд. юрид. наук: 5.1.4 / Марита Сергеевна Ремизова. – Саратов, 2025. – 319 с.

267. Рудакова С. В. Познание судом обстоятельств уголовного дела : автореф. дис. … канд. юрид. наук: 12.00.09 / Светлана Викторовна Рудакова. – Краснодар, 2004 – 23 с.

268. Рудин, А. В. Проверка доказательств в ходе досудебного производства в российском уголовном процессе: дис. ... канд. юрид. наук: 12.00.09 / Артем Владимирович Рудин. – Краснодар, 2019. – 188 с.

269. Русман, Г. С. Судебный контроль за применением мер пресечения в виде заключения под стражу, домашнего ареста : автореф. дис. … канд. юрид. наук: 12.00.09 / Галина Сергеевна Русман. – Челябинск, 2011. – 24 с.

270. Рыбин, А. В. Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации: Процессуальные и криминалистические аспекты: дис. ... канд. юрид. наук: 12.00.09 / Александр Владимирович Рыбин. – Краснодар, 2005. – 192 с.

271. Смирнов, В. Е. Гарантии прав личности в уголовном судопроизводстве в условиях цифровизации : автореф. дис. … канд. юрид. наук: 5.1.4 / Владимир Евгеньевич Смирнов. – М., 2025 – 32 с.

272. Сморгунова, М. Е. Теоретические основы и практика проверки досудебных доказательств в уголовном процессе : дис. … канд. юрид. наук: 12.00.09 / Нижний Новгород, – 2004 – 250 с.

273. Телевицкая Ю. А. Выемка электронных носителей информации по уголовным делам : дис. … канд. юрид. наук: 5.1.4 / Юлия Андреевна Телевицкая. – Нижний Новгород, – 2023. – 330 с.

Приложения

Приложение № 1

Проект

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений и дополнений
в Уголовно-процессуальный кодекс Российской Федерации

Внести в Уголовно-процессуальный кодекс Российской Федерации (Собрание законодательства Российской Федерации, 2001, № 52, ст. 4921) следующие изменения и дополнения:

1) статью 5 дополнить пунктами следующего содержания:

«14.2) контрольное значение (хэш-значение) – вычисляемое значение, используемое для проверки целостности электронных данных и подтверждения их неизменности;

14.3) криминалистическая копия (образ) – копия электронных данных, полученная способом, обеспечивающим проверяемую неизменность и воспроизводимость результата, включая фиксацию контрольных значений;

60.1) электронные данные – сведения в цифровой форме, создаваемые, обрабатываемые, передаваемые, принимаемые, хранимые или отображаемые с использованием электронных устройств, информационных систем, информационно-телекоммуникационных сетей, программного обеспечения, средств связи и иных технических средств, включая содержание сообщений, файлы, журналы событий, служебную информацию, метаданные, сетевые

идентификаторы, сведения об учетных записях, параметры передачи и иные сведения, имеющие значение для уголовного дела;

60.2) электронное доказательство – это сведения, содержащиеся в электронной среде, об обстоятельствах, имеющих значение для уголовного дела, зафиксированные средствами информационно-коммуникационных технологий в электронной форме, представленные в пригодном для восприятия человеком виде (с использованием электронных вычислительных машин и иной техники), порядок обращения которых регулируется нормами уголовно-процессуального права;

63) технический источник электронных данных – электронное устройство, электронный носитель информации, информационная система, учетная запись, сервер, облачное хранилище, информационный сервис, сеть связи, программная среда либо иной технический объект, в котором электронные данные создаются, обрабатываются, передаются, принимаются или хранятся либо из которого они получаются;

64) субъектный источник электронных данных – физическое лицо, юридическое лицо либо должностное лицо, с действиями, доступом, полномочиями или использованием которых может быть связано создание, изменение, передача, получение, хранение либо использование электронных данных;

65) производная форма электронных данных – зафиксированное в иной форме воспроизведение электронных данных, включая распечатку, скриншот, фотографию экрана, текстовую выгрузку и иное отображение электронных данных, не содержащее в полном объеме их технических характеристик.»;

2) в статье 29 часть 2 дополнить пунктом 14 следующего содержания:

«14) разрешает получение у владельца информационной системы или иного лица, располагающего такими данными содержания электронных сообщений (переписки) и иных данных, охраняемых тайной связи, в случаях, предусмотренных настоящим Кодексом.»;

3) статью 53 дополнить пунктом 8.1 следующего содержания:

8.1) получать копии предоставленных электронных данных и (или) копии образов электронных носителей информации в объеме, необходимом для проведения независимого исследования (заключения специалиста, экспертизы), при соблюдении требований о недопустимости разглашения данных предварительного расследования и принятии мер по защите персональных данных третьих лиц и иной охраняемой законом тайны;».

4) часть 2 статьи 74 дополнить пунктом 7 следующего содержания:

«7) электронные доказательства.»;

5) статью 74 дополнить частью 2.1 следующего содержания:

«2.1. Электронные сведения подлежат получению, исследованию и закреплению, в первоначальном виде из технического источника электронных данных.

Использование производной формы электронных сведений допускается в случае невозможности получения электронных сведений в первоначальном виде.

В этом случае в протоколе следственного или судебного действия указываются причины невозможности получения электронных сведений в первоначальном виде, способ получения производной формы электронных сведений, а также сведения о проверке ее соответствия полученным электронным сведения либо иным материалам уголовного дела»;

6) статью 75 дополнить частью третьей следующего содержания:

«3. Электронные данные признаются недопустимыми доказательствами, если в ходе их собирания, закрепления, хранения, передачи, исследования или проверки не обеспечена возможность установления:

1) аутентичности;

2) технического источника электронных данных, а в необходимых случаях – субъектного источника электронных данных;

3) целостности (неизменности);

4) воспроизводимости;

5) верифицируемости;

6) прослеживаемости обращения с электронными данными.

Электронные данные не могут быть признаны недопустимыми доказательствами только по мотиву отсутствия одного или нескольких признаков, указанных в настоящей части, если возможность проверки их происхождения, содержания, целостности и достоверности обеспечена иными доказательствами и процессуальными средствами, предусмотренными настоящим Кодексом»

7) статью 87 дополнить частью второй следующего содержания:

«Проверка электронных сведений осуществляется путем установления их происхождения, технических условий создания, изменения, хранения, передачи и получения, а также путем сопоставления содержащихся в них метаданных с иными доказательствами по уголовному делу и исследования условий их обнаружения, изъятия, копирования, закрепления, хранения и приобщения к уголовному делу»;

8) статью 88 дополнить частью 1.1 следующего содержания:

«1.1. При оценке электронных данных подлежат установлению:

1) относимость – с учетом содержания электронных сведений и их связи с обстоятельствами, подлежащими доказыванию, в том числе по техническим параметрам;

2) допустимость – с учетом соблюдения требований настоящего Кодекса при их обнаружении, изъятии, копировании, закреплении, хранении и приобщении к уголовному делу;

3) достоверность – с учетом целостности, происхождения, аутентичности электронных данных, отсутствия признаков их изменения, а также проверки условий формирования содержащихся в них метаданных.

Временные метки, геолокационные данные и иные метаданные не могут признаваться достоверными без проверки условий их формирования и сопоставления с иными доказательствами по уголовному делу»;

9) статью 164 дополнить частью шестой.1 следующего содержания:

6.1. Осмотр электронных устройств и электронных носителей информации производится, если иное не обусловлено обстоятельствами уголовного дела, в условиях, исключающих изменение электронных данных вследствие

автоматического подключения к информационно-телекоммуникационным сетям, удаленного доступа, синхронизации, автоматического обновления либо иных технических процессов.

В случае отступления от указанного требования причины и характер такого отступления подлежат обязательному отражению в протоколе»;

10) В статье 164.1:

а) часть первую изложить в следующей редакции: «1. Изъятие электронных носителей информации, копирование содержащихся на них электронных данных, доступ к электронным данным, их фиксация, упаковка, опечатывание, хранение и передача осуществляются с соблюдением требований, обеспечивающих целостность электронных данных, возможность проверки их происхождения и неизменности»;

б) дополнить частями 1.1–1.3 следующего содержания:

«1.1. Участие специалиста обязательно:

1) при необходимости преодоления средств защиты, шифрования, аутентификации или иных технических ограничений доступа;

2) при копировании, извлечении либо фиксации электронных данных с использованием специальных программно-технических средств;

3) при создании цифрового образа электронного носителя информации;

4) при работе с серверным, сетевым, виртуальным, облачным либо иным технически сложным объектом;

5) при наличии риска утраты, изменения либо уничтожения электронных данных в ходе следственного действия.

1.2. Для целей настоящей статьи технически сложным является объект или ситуация, при которых получение, фиксация, копирование, сохранение или исследование электронных данных требует использования специальных знаний, специальных технических средств либо связано с риском утраты, изменения или уничтожения электронных данных.

1.3. В случае непривлечения специалиста при производстве следственного действия, связанного с получением, фиксацией, изъятием, копированием либо

исследованием электронных данных, следователь или дознаватель обязан указать мотивы такого решения в протоколе либо постановлении»

в) дополнить частью 3.1 следующего содержания: «3.1. При изъятии, копировании и закреплении электронных данных в протоколе указываются способ доступа к ним, примененные технические средства и программное обеспечение, последовательность действий, сведения о создании копии или цифрового образа, а также контрольные значения либо иные сведения, подтверждающие целостность полученных электронных данных»;

г) дополнить частями 4-6 следующего содержания:

«4. Копии электронных данных и материалы, необходимые для их проверки, предоставляются подозреваемому, обвиняемому, защитнику, а также потерпевшему, гражданскому истцу, гражданскому ответчику и их представителям по их ходатайству, если предоставление таких копий и материалов не создает угрозу охраняемой федеральным законом тайне, правам и законным интересам иных лиц, а также безопасности участников уголовного судопроизводства.

Ограничение в предоставлении указанных копий и материалов допускается только на основании мотивированного постановления следователя, дознавателя либо определения суда и может быть обжаловано в порядке, установленном настоящим Кодексом;

5. При производстве следственных действий, связанных с обнаружением, изъятием, осмотром, копированием, сохранением электронных носителей информации и содержащихся на них электронных данных, дознаватель, следователь вправе получать доступ, фиксировать, копировать и изымать только те электронные данные, которые имеют значение для уголовного дела и относятся к обстоятельствам, подлежащим доказыванию. Не допускаются собирание, копирование, исследование, изъятие и приобщение к материалам уголовного дела электронных данных, заведомо не относящихся к уголовному делу, а равно данных о частной жизни лица и иных лиц, не связанных с расследуемым событием, за исключением случаев, предусмотренных настоящим Кодексом.

6. Осмотр и исследование электронных данных, локально содержащихся в памяти законно изъятого электронного устройства или иного электронного носителя информации, допускаются без получения судебного решения в порядке, установленном настоящим Кодексом. Доступ к удаленным электронным данным, осуществляемый с использованием законно изъятого электронного устройства или иного электронного носителя информации, а равно получение электронных данных, находящихся у оператора связи, провайдера либо иного лица, обеспечивающего хранение, обработку, передачу или предоставление электронных сообщений и иной электронной информации, допускаются на основании судебного решения, за исключением случаев, не терпящих отлагательства, предусмотренных статьей 186.3 настоящего Кодекса.»;

11) В статье 166

а) дополнить частью 3.1. следующего содержания:

«3.1. В протоколе следственного действия, связанного с обнаружением, осмотром, изъятием, копированием или исследованием электронных данных, указываются:

1) вид, наименование, модель, серийный номер электронного устройства либо иные индивидуализирующие признаки электронного объекта;

2) характеристики электронного носителя информации;

3) сведения об учетной записи пользователя, если они установлены;

4) место расположения файла, электронного объекта либо совокупности электронных данных;

5) наименование, формат, размер, дата и время создания, изменения и последнего доступа к электронным данным, если такие сведения доступны;

6) используемое программное обеспечение;

7) способ доступа к электронным данным;

8) сведения о подключении устройства к информационно-телекоммуникационной сети либо об его отключении от такой сети;

9) сведения о наличии паролей, средств защиты и шифрования;

10) последовательность действий по обнаружению, извлечению, копированию и закреплению электронных данных;

11) сведения о лицах, осуществлявших соответствующие действия;

12) способ копирования и использованные технические средства;

13) контрольные значения либо иные результаты проверки целостности электронных данных;

14) сведения об упаковке, опечатывании и передаче объекта на хранение;

15) сведения о приложениях к протоколу»;

б) дополнить частью восемь.1 следующего содержания:

«8.1. Приложения к протоколу следственного действия, содержащие электронные носители информации, копии электронных данных, цифровые образы носителей информации, распечатки, скриншоты, фототаблицы и иные материалы, подлежат подписанию, упаковке, маркировке и хранению в порядке, обеспечивающем их индивидуализацию, сохранность и возможность проверки их происхождения и неизменности»;

12) статью 177 дополнить частями 3.1, 3.2 и 7 следующего содержания:

«3.1. При осмотре электронного устройства подлежат разграничению электронные данные, содержащиеся в памяти устройства, и электронные данные, получаемые посредством удаленного доступа, синхронизации либо взаимодействия с внешними информационными системами.

3.2. В протоколе осмотра электронного устройства указывается, какие электронные данные получены из памяти устройства, а какие — посредством удаленного доступа, синхронизации либо взаимодействия с внешними информационными системами, с указанием способа их получения.

7. При осмотре электронного устройства или иного электронного носителя информации в протоколе осмотра подлежат обязательному отражению сведения об индивидуализирующих признаках устройства или носителя информации, условиях, последовательности и способе доступа к электронным данным, примененных технических средствах и программном обеспечении, действиях по поиску, обнаружению, просмотру, копированию, сохранению и фиксации

электронной информации, а также сведения, позволяющие проверить целостность, происхождение и неизменность полученных электронных данных.»;

13) дополнить статьей 185.1 следующего содержания:

«Статья 185.1. Безотлагательное сохранение электронных данных

1. В целях предотвращения утраты, уничтожения, изменения либо перезаписи электронных данных, имеющих значение для уголовного дела, следователь, дознаватель вправе принять меры к безотлагательному сохранению электронных данных, если имеются достаточные данные полагать, что отсутствует реальная возможность их изъятия, а промедление может повлечь невозможность их последующего получения и проверки.

2. Безотлагательное сохранение электронных данных допускается в отношении электронных сведений, находящихся у операторов связи, владельцев сервисов и информационных систем, провайдеров облачного хранения, хостинг-провайдеров, администраторов корпоративных систем и иных организаций, владеющих либо распоряжающихся соответствующими данными.

3. Безотлагательное сохранение электронных данных производится на основании постановления следователя, дознавателя, в котором указываются: номер уголовного дела и обоснование необходимости безотлагательного сохранения; адресат постановления (наименование, реквизиты); перечень электронных данных, подлежащих безотлагательному сохранению, с максимально возможной конкретизацией объема электронных данных, включая идентификаторы электронных объектов (аккаунта, абонента, учетной записи, ресурса, сообщения, файла либо иные идентификаторы в зависимости от вида системы), временной интервал и часовой пояс их местонахождения, категорию и объем электронных данных; срок обеспечения сохранности электронных данных; предупреждение об ответственности за неисполнение законного требования адресатом вышеуказанного постановления следователя, дознавателя о безотлагательном сохранении электронных данных.

4. Адресат постановления обязан безотлагательно обеспечить сохранение указанных электронных данных и исключить их удаление, изменение

и перезапись в пределах указанного объема; ограничить доступ к сохраненным данным и исключить их модификацию в результате штатных процедур хранения; оформить документ об исполнении, в котором указываются дата и время исполнения постановления, уполномоченное лицо, способ обеспечения сохранности электронных данных, перечень сохраненных категорий данных, временной интервал и часовой пояс местонахождения, а также внутренний идентификатор сформированного архива (снимка, выгрузки); при технической возможности указать контрольные значения (хэш) сформированного архива (либо ключевых файлов) и обеспечить учет обращений к сохраненным данным.

5. Следователь, дознаватель составляет протокол обеспечения сохранности электронных данных, в котором отражаются сведения о вынесении и направлении постановления о безотлагательном сохранении электронных данных, способ направления указанного постановления, сведения об адресате, содержание требований, полученные документы об исполнении и иные данные, необходимые для последующей проверки происхождения и неизменности сохраненного объема электронных данных. Документы адресата приобщаются к материалам уголовного дела.

6. Срок обеспечения сохранности электронных данных не может превышать 30 суток. Продление срока допускается по судебному решению в порядке, предусмотренном ст. 165 УПК РФ.

7. Обеспечение сохранности электронных данных не является предоставлением следователю, дознавателю доступа к их содержанию. Получение сохраненных электронных данных осуществляется в порядке, предусмотренном настоящим Кодексом, с соблюдением требований, установленных федеральным законом.

14) дополнить статьей 186.2 следующего содержания:

«Статья 186.2. Получение электронных данных у владельца информационной системы или иного лица, располагающего такими данными

1. Следователь или дознаватель вправе получать электронные данные, имеющие значение для уголовного дела, у владельца информационной системы,

владельца сервиса, оператора связи, провайдера, хостинг-провайдера, владельца облачной инфраструктуры либо иного лица, располагающего такими данными, в порядке, установленном настоящей статьей.

2. В требовании о предоставлении электронных данных указываются: сведения об уголовном деле; лицо или организация, которым адресовано требование; перечень запрашиваемых электронных данных; идентификаторы учетной записи, абонента, ресурса, устройства, сообщения, файла либо иные идентификаторы, если они известны; период, за который запрашиваются электронные данные, с указанием временного интервала и часового пояса, если это необходимо; форма предоставления электронных данных; необходимость приложения сведений, подтверждающих происхождение электронных данных, условия их формирования, параметры выборки, способ передачи и сведения, подтверждающие их целостность.

3. Получение содержания сообщений, переписки, переговоров и иных сведений, составляющих тайну связи либо иную охраняемую федеральным законом тайну, допускается на основании судебного решения, за исключением случаев, предусмотренных настоящим Кодексом.

4. Лицо, исполняющее требование, обязано указать источник формирования предоставляемых электронных данных, способ и дату их выгрузки, параметры выборки, временной интервал и часовой пояс, если они определялись, сведения о целостности данных, контрольные значения файлов либо архива, а также иные сведения, имеющие значение для проверки их происхождения и неизменности.

5. Полученные электронные данные подлежат осмотру приобщению к материалам уголовного дела с приложением документов и материалов, подтверждающих их происхождение, способ передачи и целостность.

6. При наличии риска утраты либо изменения электронных данных до их получения могут быть приняты меры к их безотлагательному сохранению в порядке, предусмотренном статьей 185.1 настоящего Кодекса.»;

15) дополнить Кодекс статьей 186.3 следующего содержания:

«Статья 186.3. Получение удаленных электронных данных

1. При наличии достаточных оснований полагать, что удаленные электронные данные содержат сведения, имеющие значение для уголовного дела, и доступ к таким данным возможен с использованием изъятого электронного устройства, иного электронного носителя информации, следователь с согласия руководителя следственного органа, а дознаватель с согласия прокурора возбуждает перед судом ходатайство о разрешении получения, осмотра, копирования и сохранения таких данных.

2. В ходатайстве о производстве действий, предусмотренных частью первой настоящей статьи, указываются: наименование уголовного дела; основания полагать, что удаленные электронные данные содержат сведения, имеющие значение для уголовного дела; вид удаленных электронных данных, предполагаемый источник их нахождения и способ получения доступа к ним; обстоятельства, подтверждающие необходимость получения указанных данных; срок, в течение которого необходимо осуществить получение, осмотр, копирование и сохранение удаленных электронных данных.

3. Рассмотрев ходатайство, судья выносит постановление о разрешении получения, осмотра, копирования и сохранения удаленных электронных данных либо об отказе в производстве указанных действий.

4. На основании судебного решения следователь, дознаватель вправе осуществить получение, осмотр, копирование, закрепление и сохранение удаленных электронных данных в объеме, необходимом для достижения целей уголовного судопроизводства и не превышающем пределы, обусловленные обстоятельствами, подлежащими доказыванию.

5. В случаях, не терпящих отлагательства, когда существует реальная опасность утраты, уничтожения, изменения, блокирования либо автоматического удаления удаленных электронных данных, следователь, дознаватель вправе произвести действия, предусмотренные частью первой настоящей статьи, без предварительного судебного решения, о чем в течение 24 часов с момента начала

их производства уведомляет судью и прокурора с приложением копий постановления о производстве указанных действий и протокола их производства.

6. Проверив законность, обоснованность и соразмерность произведенных действий, судья выносит постановление о признании их законными либо незаконными. В случае признания произведенных действий незаконными полученные удаленные электронные данные признаются недопустимыми доказательствами в порядке, установленном настоящим Кодексом.

7. При производстве действий, предусмотренных настоящей статьей, не допускаются получение, копирование, исследование и использование удаленных электронных данных, заведомо не относящихся к уголовному делу, за исключением случаев выявления сведений о признаках иного преступления, подлежащих фиксации в объеме, необходимом для решения вопроса в порядке, установленном настоящим Кодексом.».

16) статью 217 дополнить частью 7 следующего содержания: «7. При ознакомлении с материалами уголовного дела стороне защиты обеспечивается доступ к электронным доказательствам в виде, позволяющем проверить их содержание и целостность, включая доступ к контрольным значениям (хэш-суммам), сведениям о примененных средствах извлечения и фиксации.».

17) статью 240 дополнить частью 1.1 следующего содержания:

«1.1. При исследовании доказательств, содержащих электронные данные, суд при наличии технической возможности обеспечивает воспроизведение аудио- и видеозаписей, демонстрацию электронных файлов либо исследование электронного носителя информации или его цифрового образа.

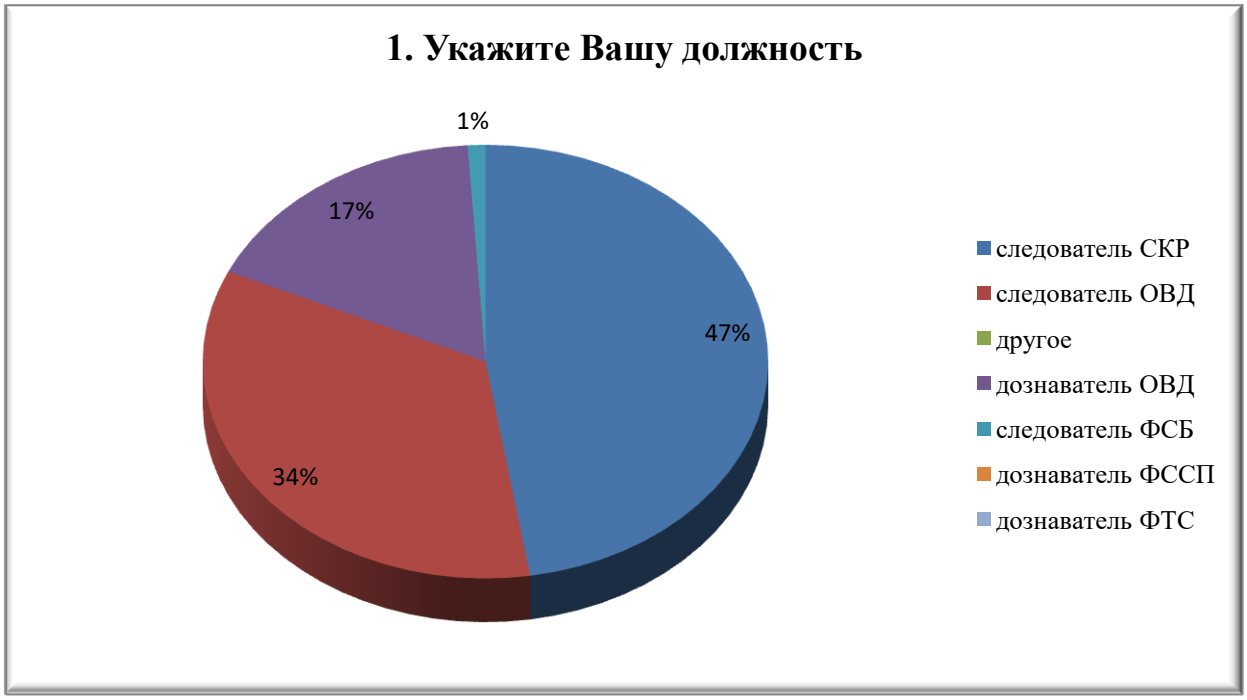
Исследование протоколов, распечаток, скриншотов и иных производных форм электронных данных не исключает непосредственного исследования электронных данных, если такое исследование возможно.».

Президент

Российской Федерации В.В. Путин

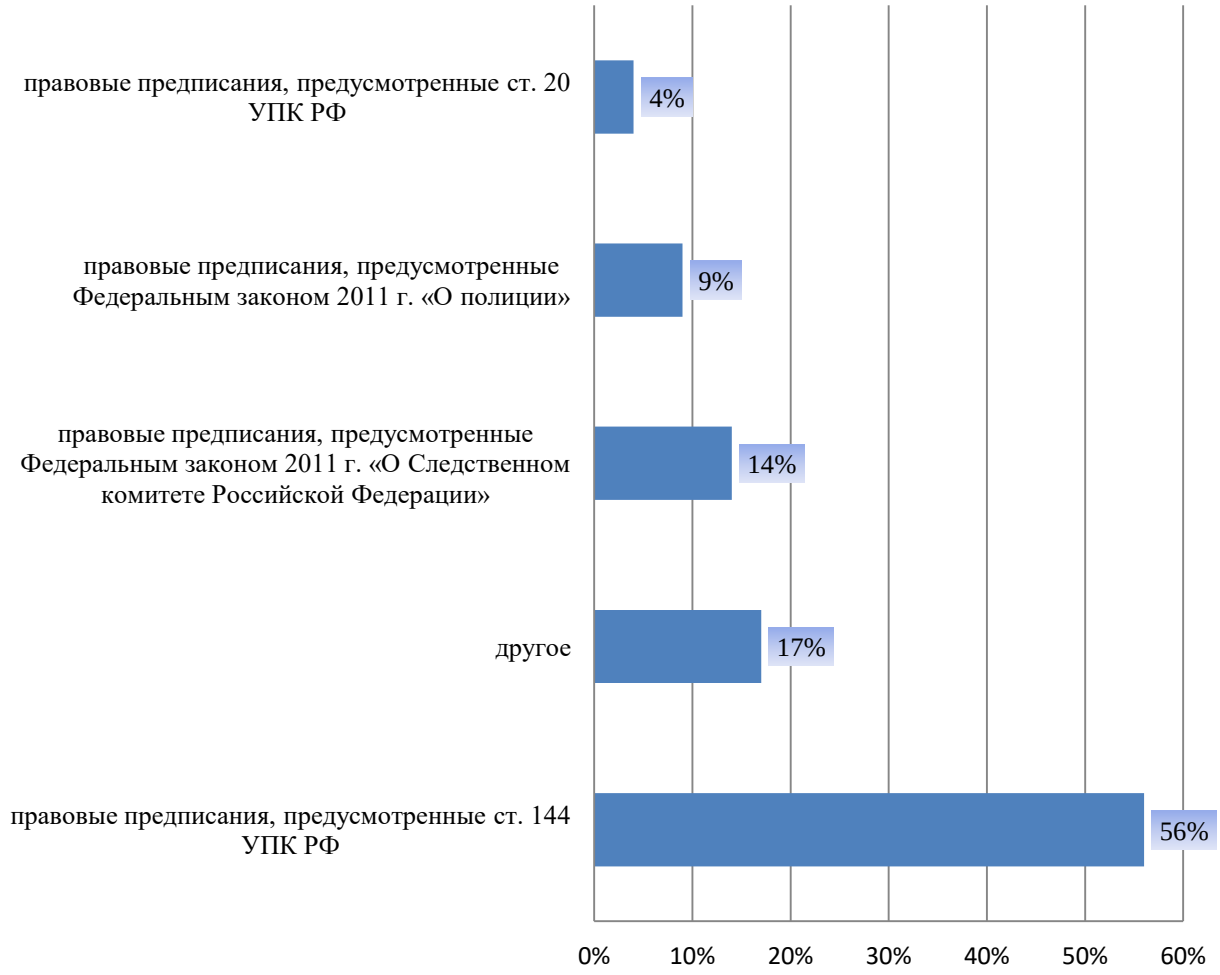
Приложение 2.

Результаты изучения мнения должностных лиц органов предварительного расследования по проблемам использования электронных доказательств в уголовном судопроизводстве

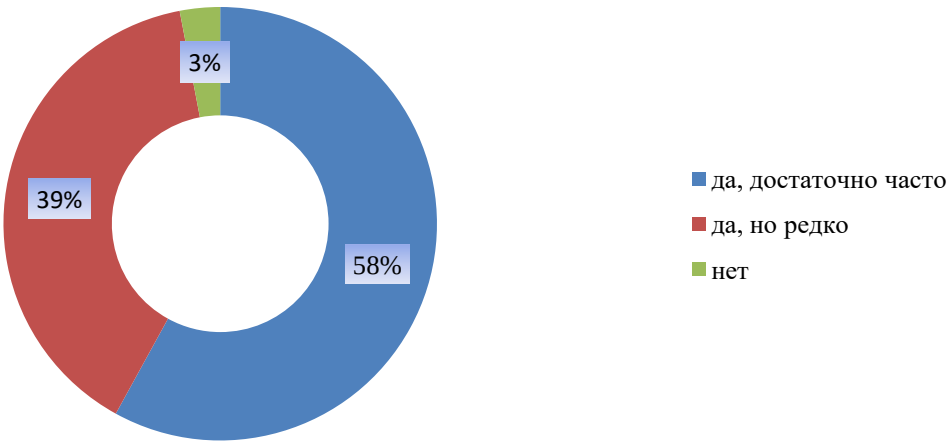




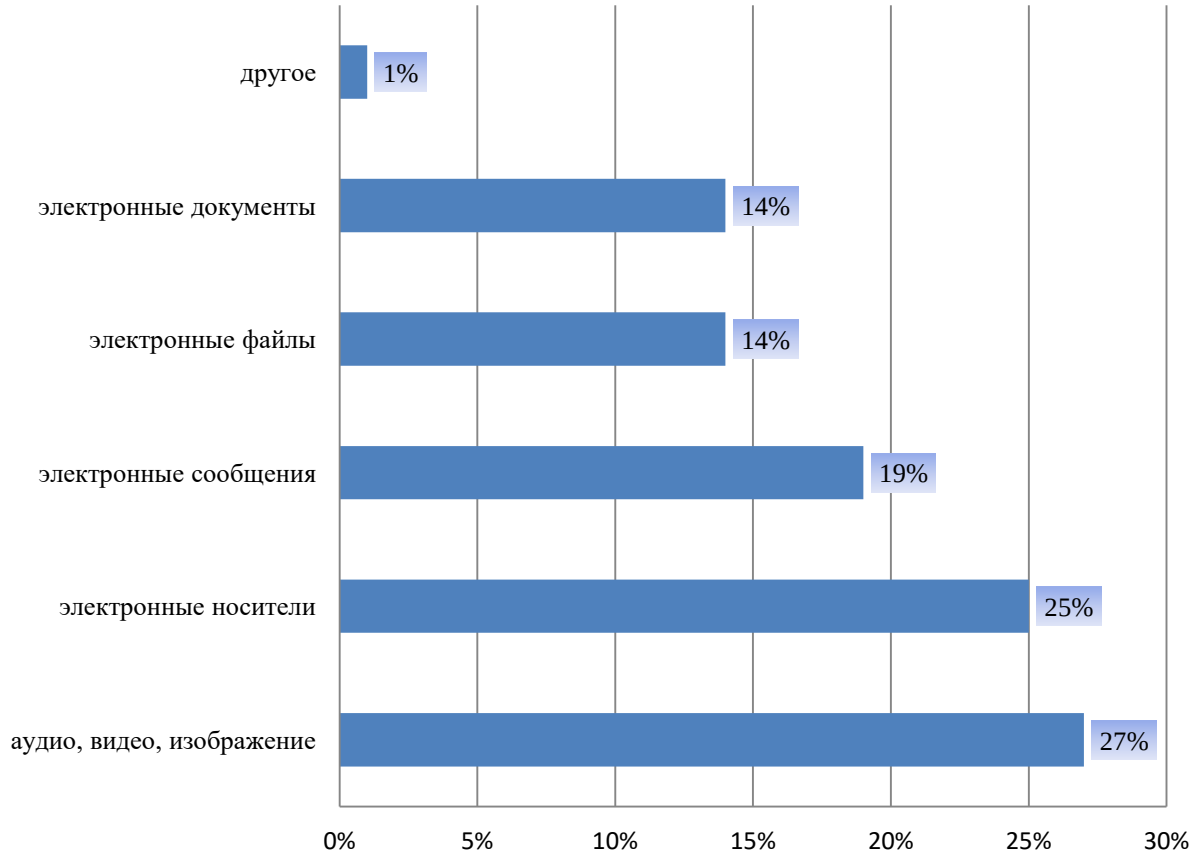
3. Каковы правовые основания истребования электронных доказательств в ходе доследственной проверки



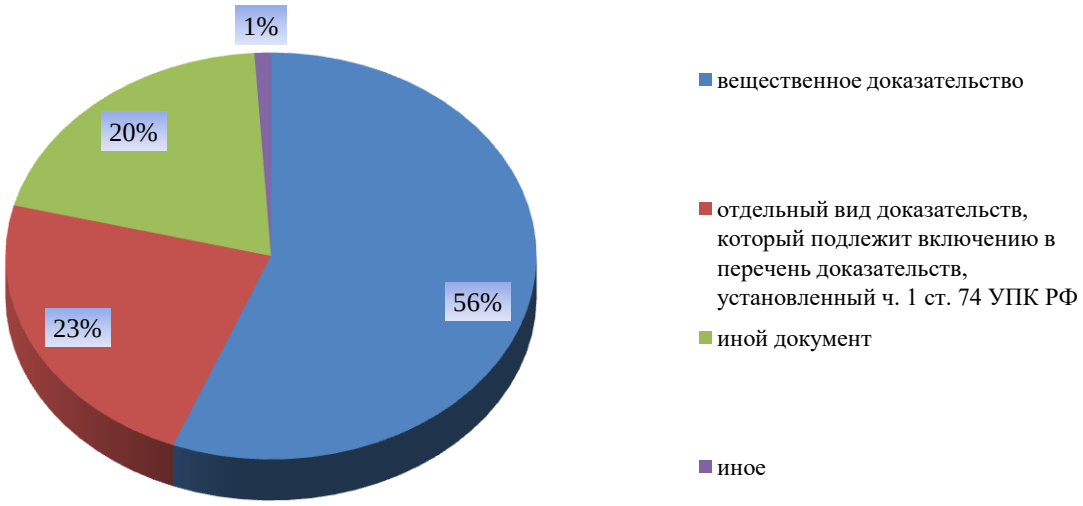
4. Используете ли Вы в доказывании по уголовным делам электронные доказательства?



5. Каковы правовые основания истребования электронных доказательств в ходе доследственной проверки

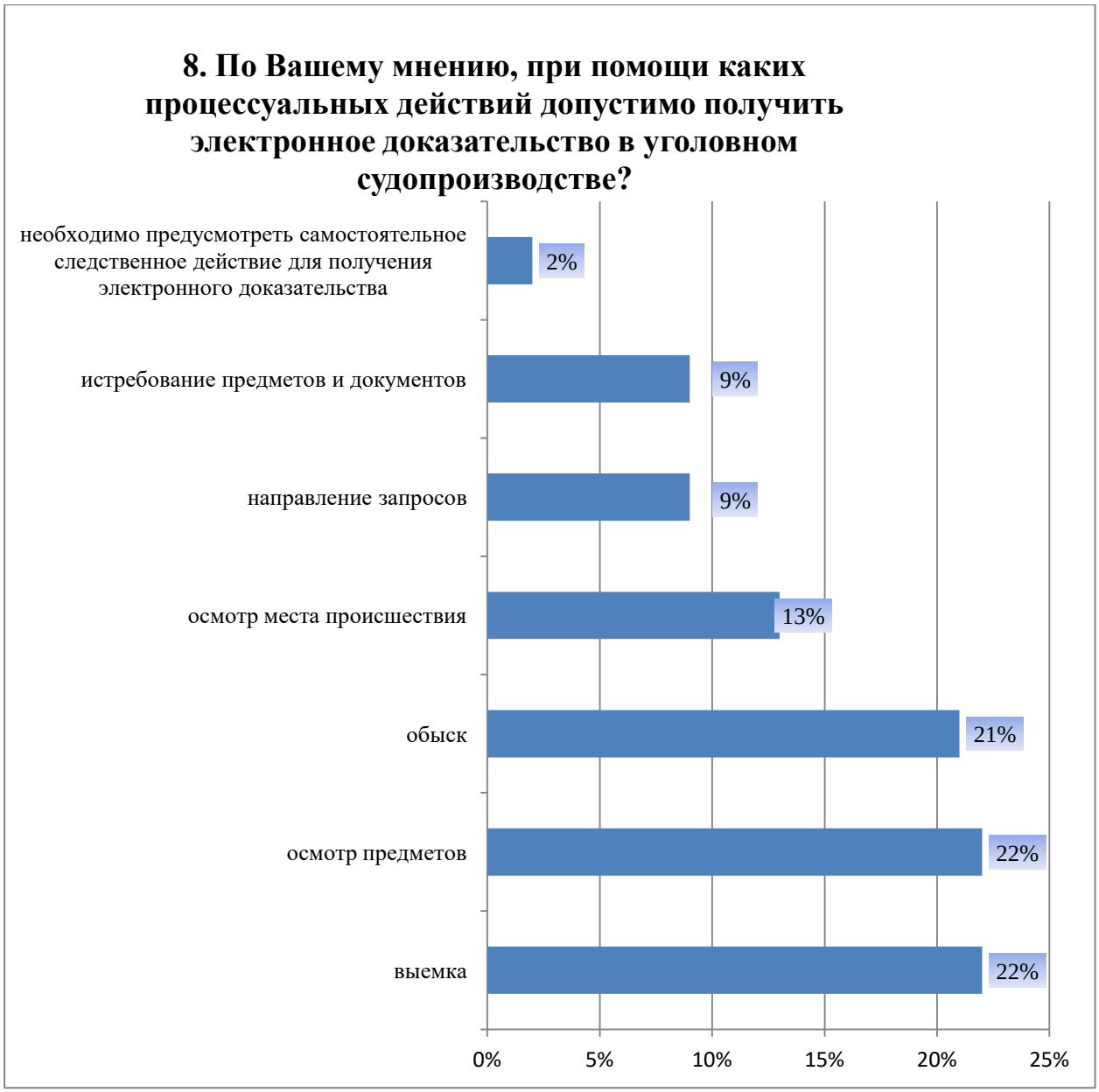


6. По Вашему мнению, каким видом доказательства по уголовному делу следует рассматривать электронное доказательство?

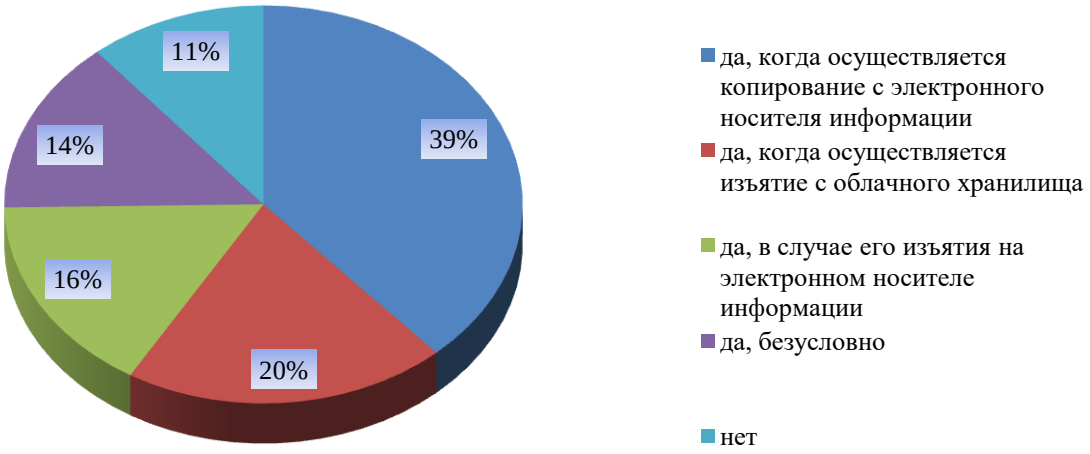


7. Требуется ли, по Вашему мнению, легализация понятия «электронное доказательство» с закреплением в ст. 5 УПК РФ?

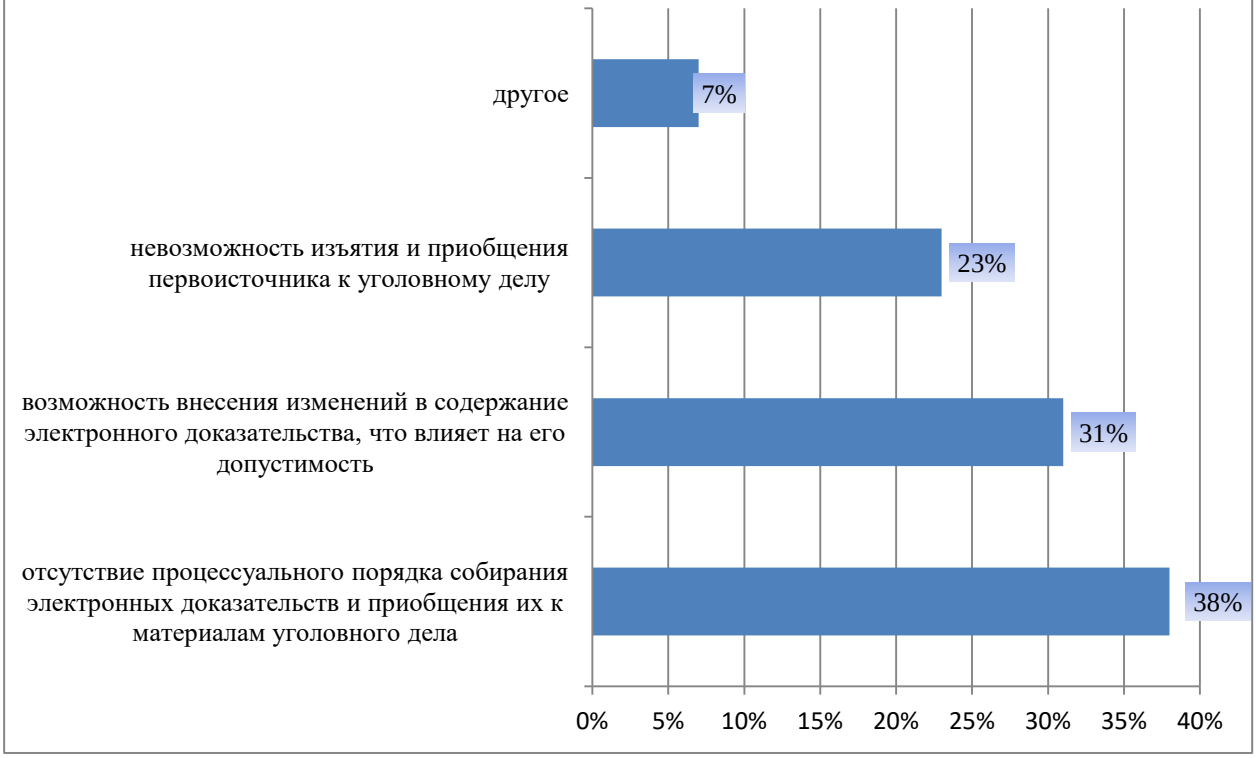



8. По Вашему мнению, при помощи каких процессуальных действий допустимо получить электронное доказательство в уголовном судопроизводстве?
необходимо предусмотреть самостоятельное следственное действие для получения электронного доказательства
2%
истребование предметов и документов
9%
направление запросов
9%
осмотр места происшествия
13%
обыск
21%
осмотр предметов
22%
выемка
22%
0%
5%
10%
15%
20%
25%

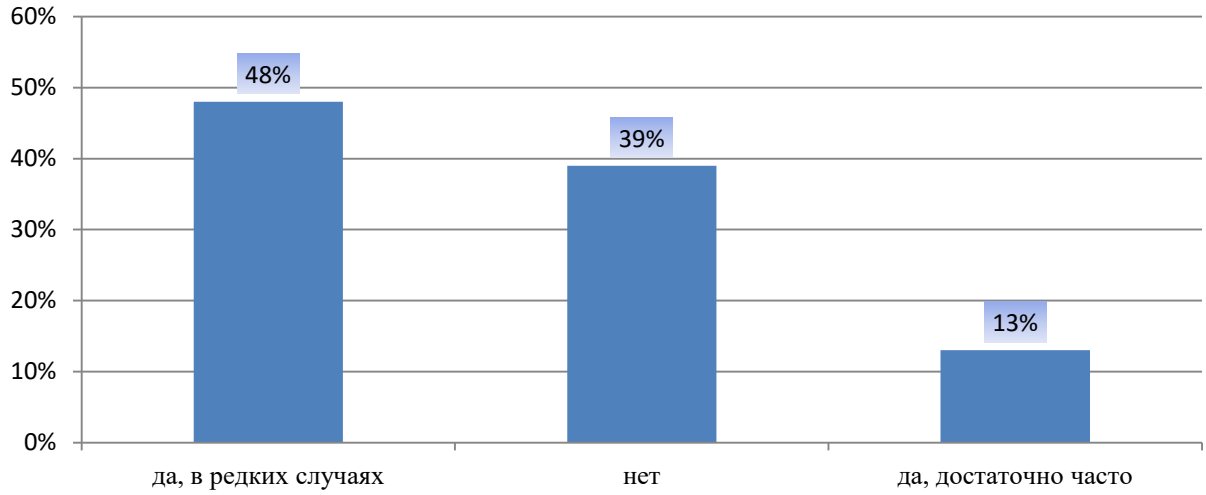
9. Привлекаете ли Вы, в ходе собирания электронных доказательств в досудебном уголовном судопроизводстве специалиста?



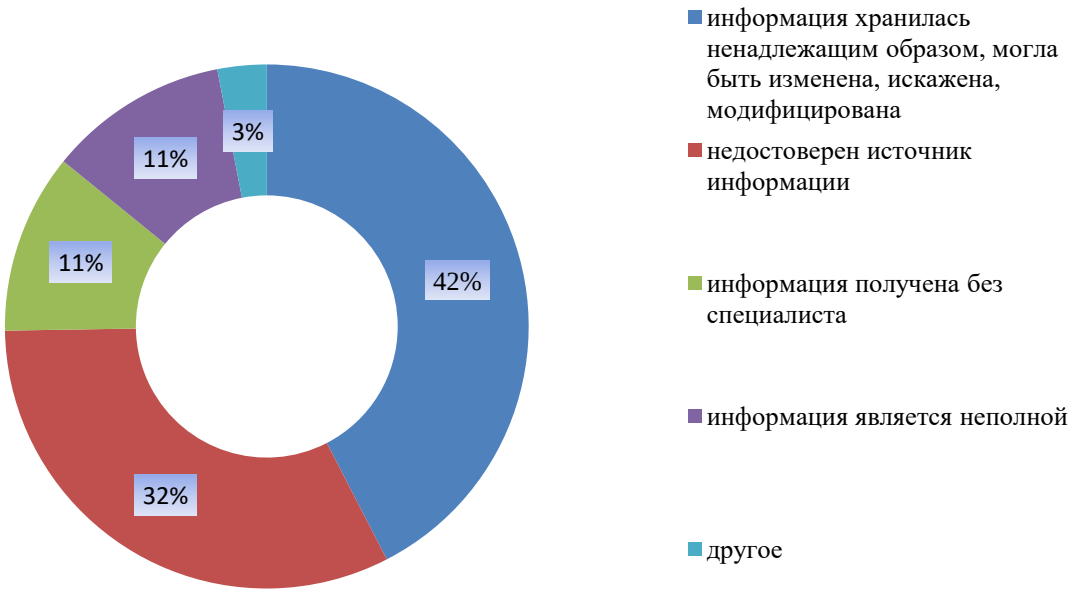
10. Какие сложности возникают в ходе собирания электронных доказательств в досудебном уголовном судопроизводстве?



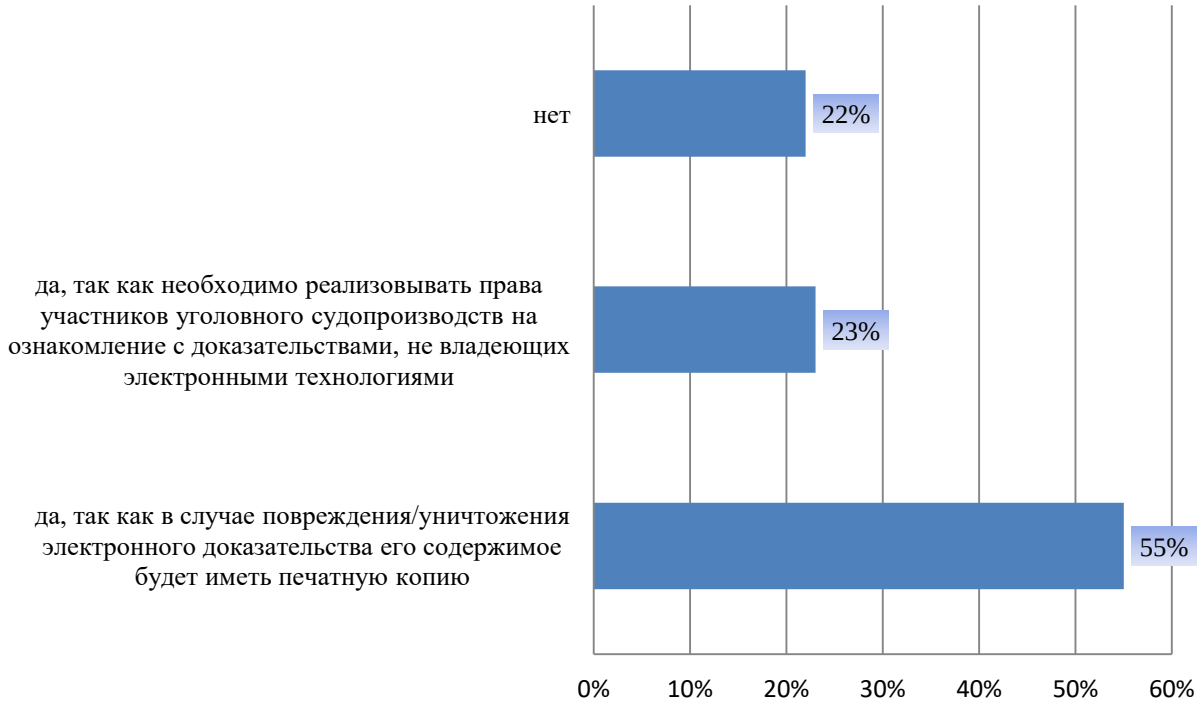
11. Заявляет ли сторона защиты ходатайства о приобщении к уголовному делу в порядке ст. 86 УПК РФ электронных материалов?



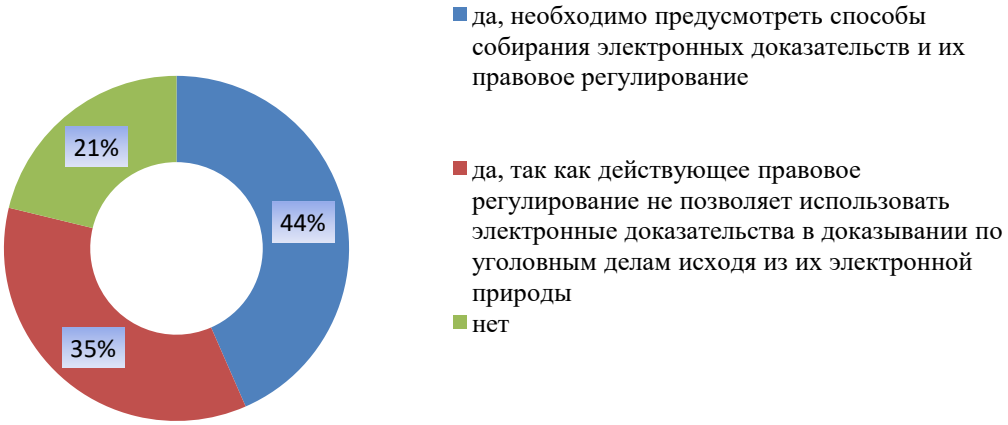
12. По Вашему мнению, какие сомнения могут возникнуть при проверке и оценке электронного доказательства?



13. Распечатываете ли Вы и приобщаете к материалам уголовного дела содержание электронного доказательства?



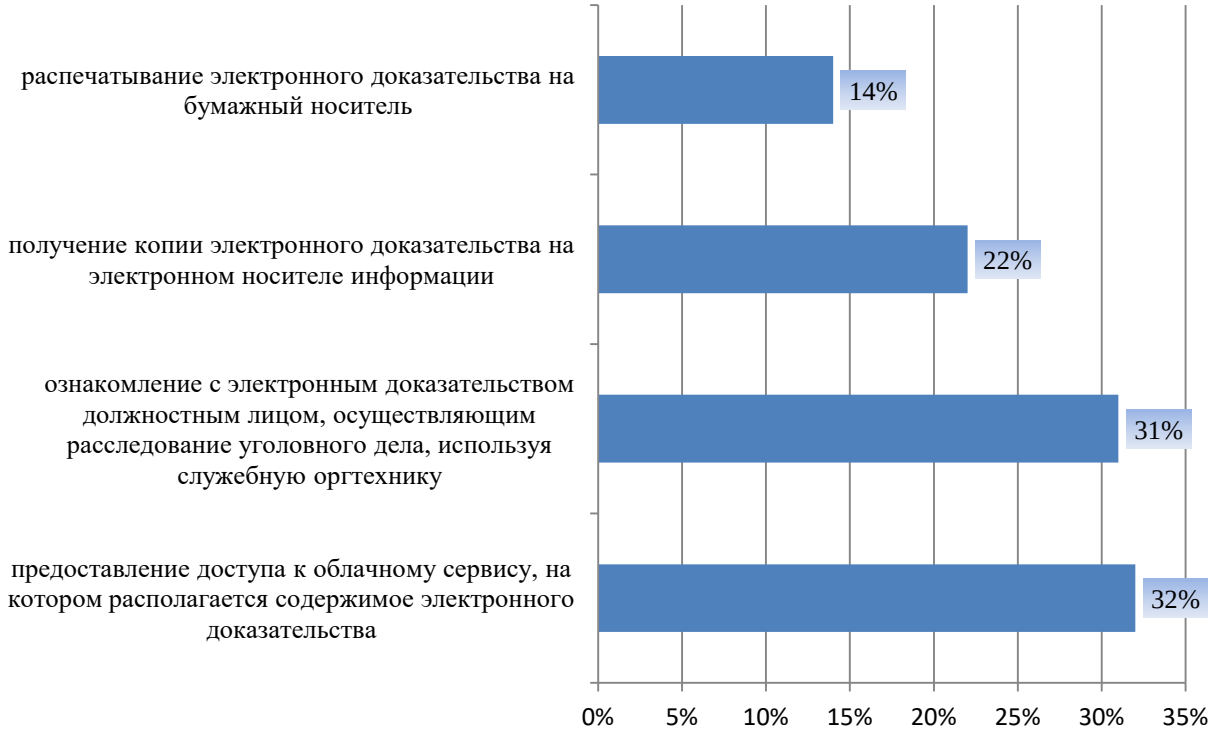
14.Считаете ли Вы, что имеется необходимость в оптимизации уголовно-процессуального законодательства в целях создания правовых условий использования электронных доказательств при исследовании обстоятельств совершенного преступления?



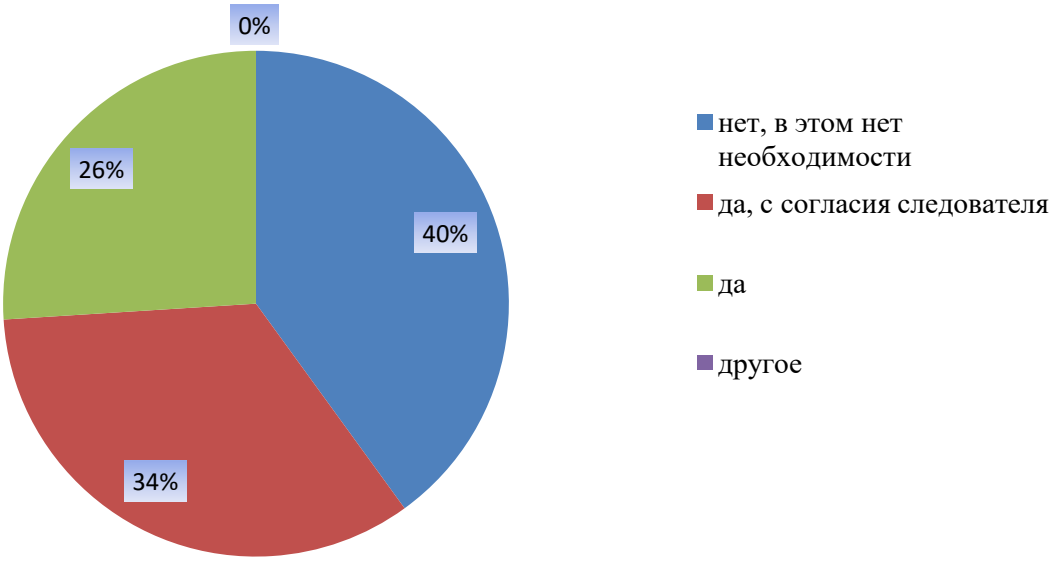
15. По Вашему мнению, необходимо ли определение дополнительных критериев допустимости для электронных доказательств?



16. Какой порядок ознакомления с электронным доказательством в ходе ознакомления с материалами уголовного дела, Вы считаете оптимальным?

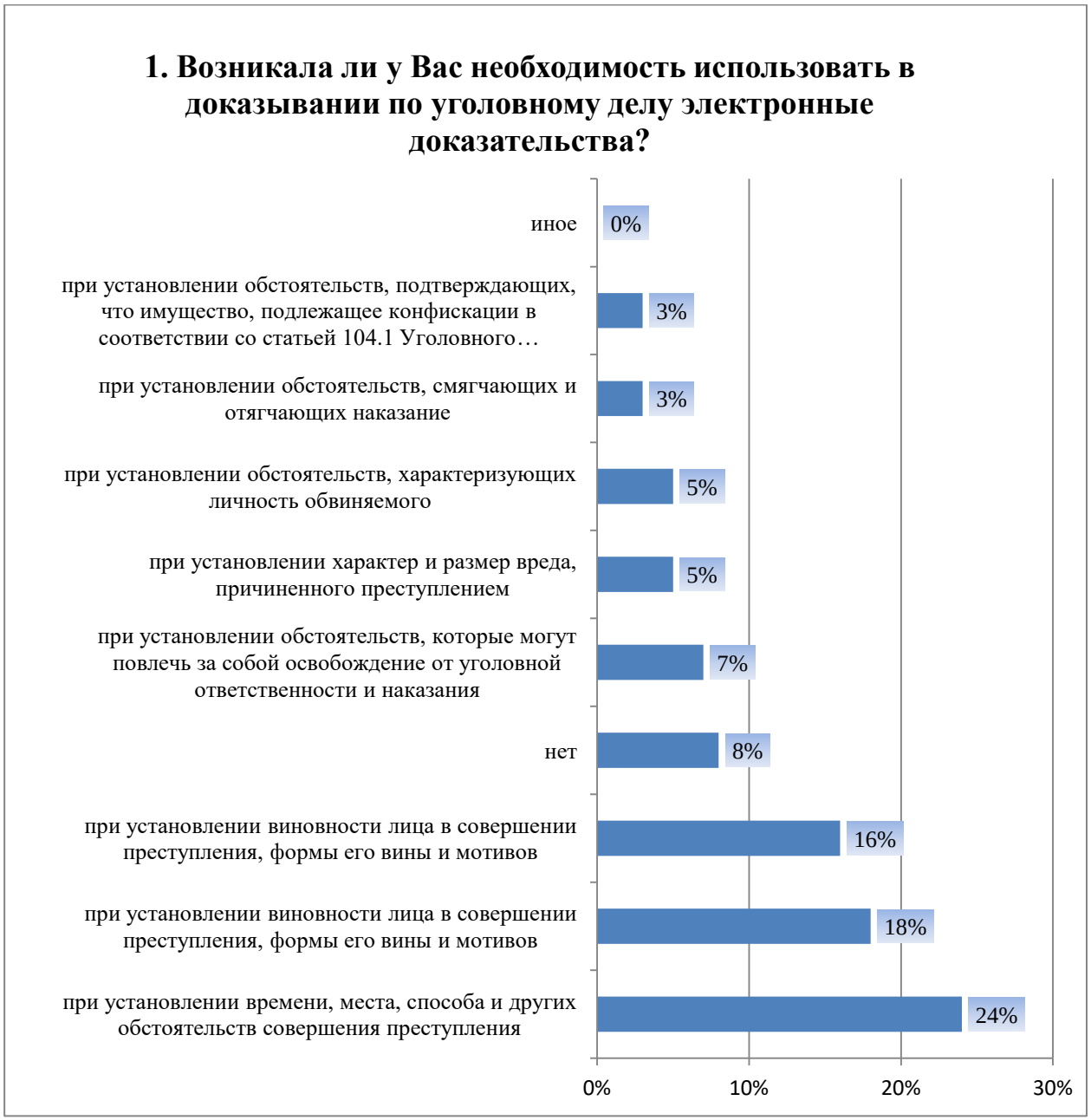


17. По Вашему мнению, необходимо ли в УПК РФ предусмотреть дополнительную гарантию прав стороны защиты – возможность приглашать специалиста для ознакомления с материалами уголовного дела в порядке ст. 217 УПК РФ для оказания технической помощи при изучени

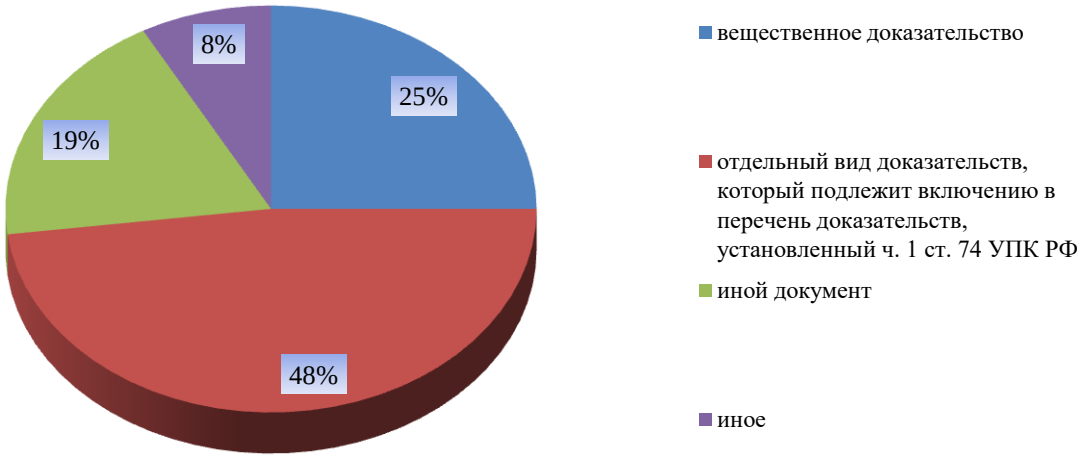


Приложение 3.

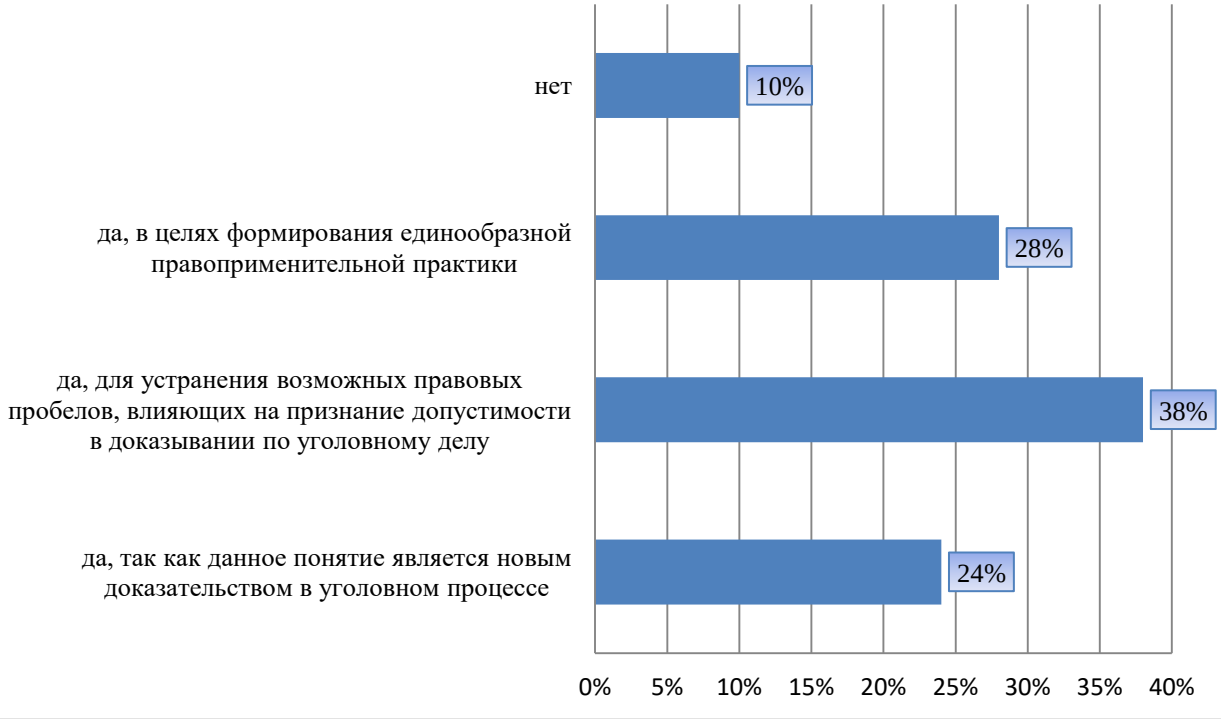
Результаты изучения мнения адвокатов-защитников по проблемам использования электронных доказательств в уголовном судопроизводстве



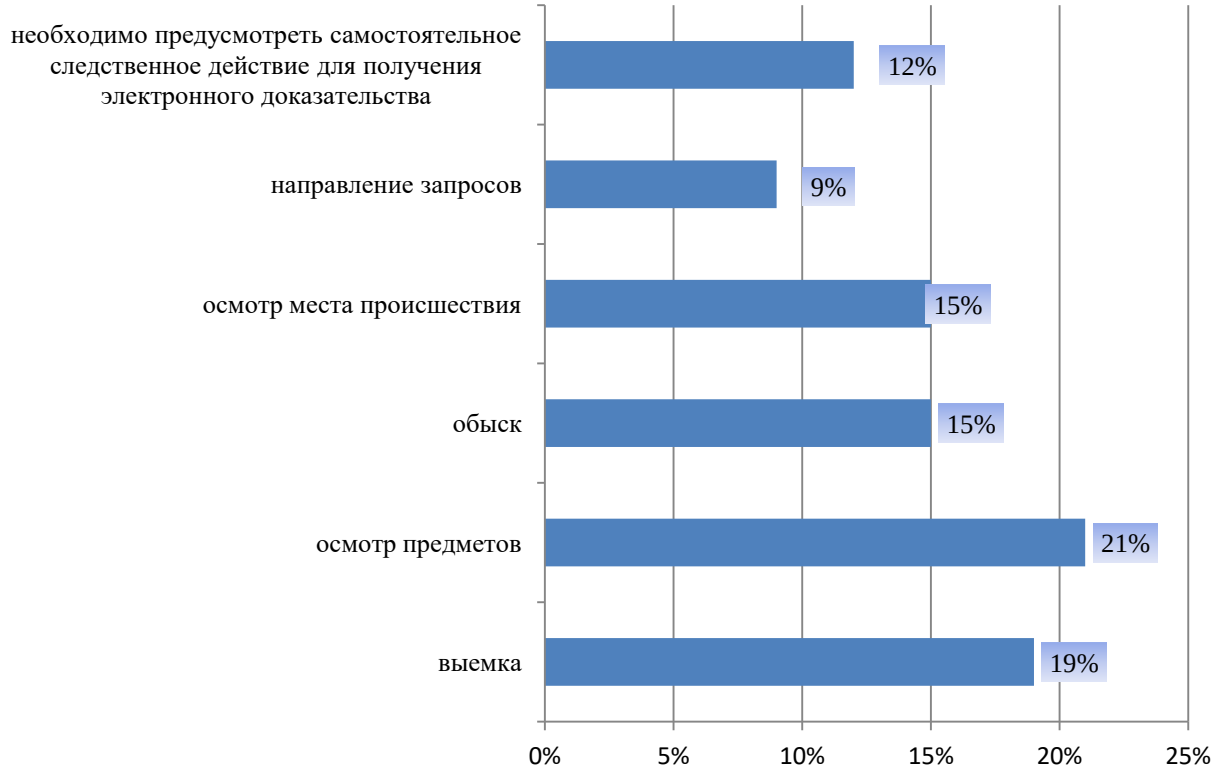
2. По Вашему мнению, каким видом доказательства по уголовному делу следует рассматривать электронное доказательство?



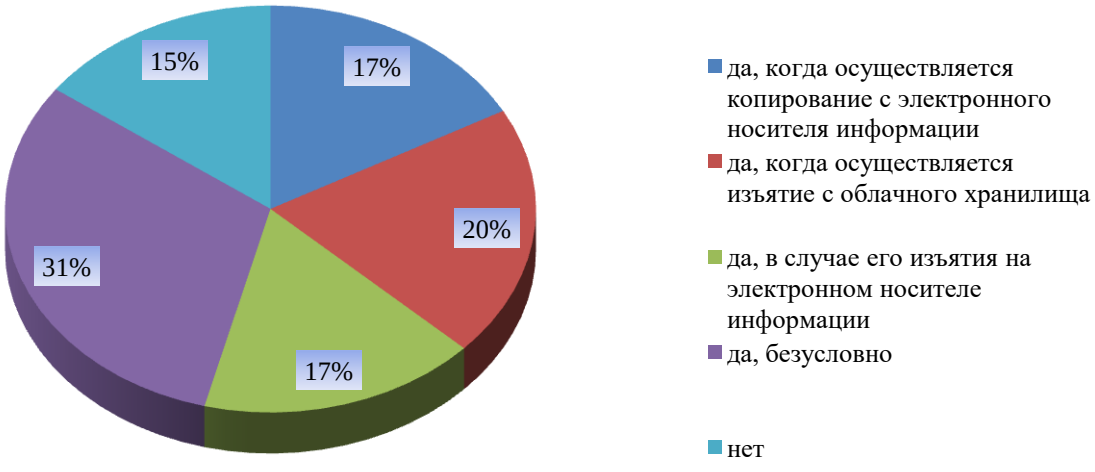
3. Требуется ли, по Вашему мнению, легализация понятия «электронное доказательство» с закреплением в ст. 5 УПК РФ?



4. По Вашему мнению, при помощи каких процессуальных действий допустимо получить электронное доказательство в уголовном судопроизводстве?



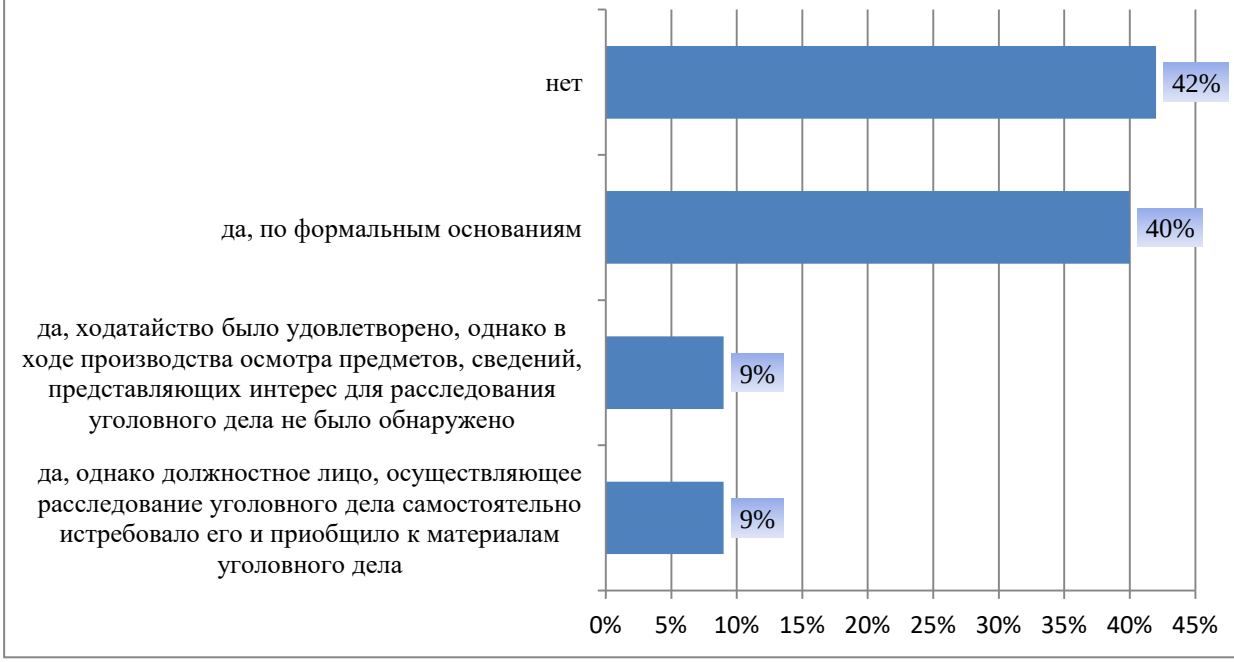
5. Считаете ли Вы, что при получении электронного доказательства в досудебном уголовном производстве необходимо привлекать специалиста?



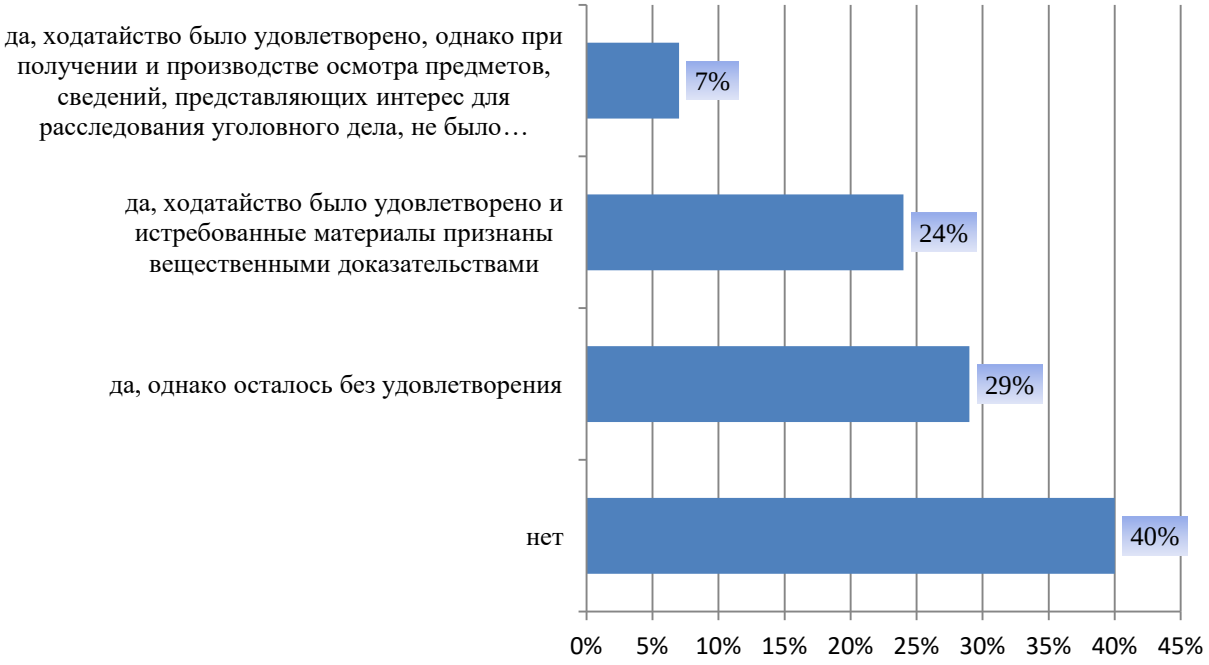
6. Какие сложности имеются у адвокатов-защитников при осуществлении защиты по уголовным делам в части собирания и предоставления электронного материала с перспективой признания их доказательством по уголовному делу?



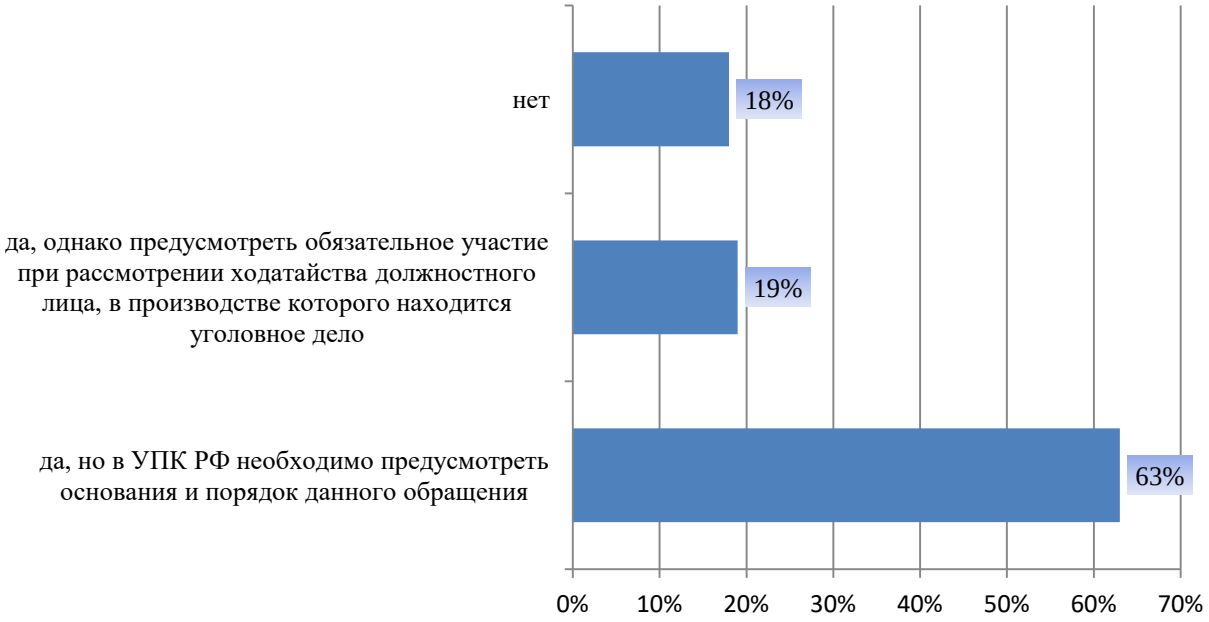
7. Имелись ли в Вашей практике случаи отказа адвокату-защитнику в приобщении электронного материала для признания в качестве доказательства по уголовному делу?



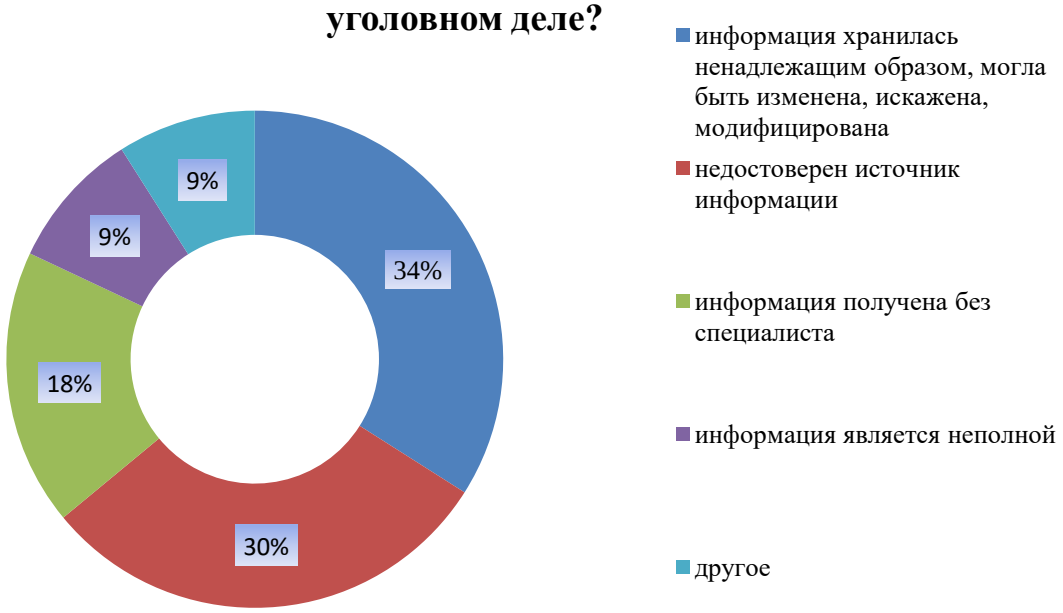
8. Вами в ходе досудебного производства по уголовному делу направлялись ходатайства должностному лицу, осуществляющему расследование уголовного дела, об истребовании электронных материалов, перечень которых ограничен законодательством в получении?



9. По Вашему мнению, необходимо ли разрешить адвокату-защитнику непосредственно обращаться в суд для получения разрешения об истребовании электронных доказательств, которые законом допускается предоставлять только при наличии судебного решения?



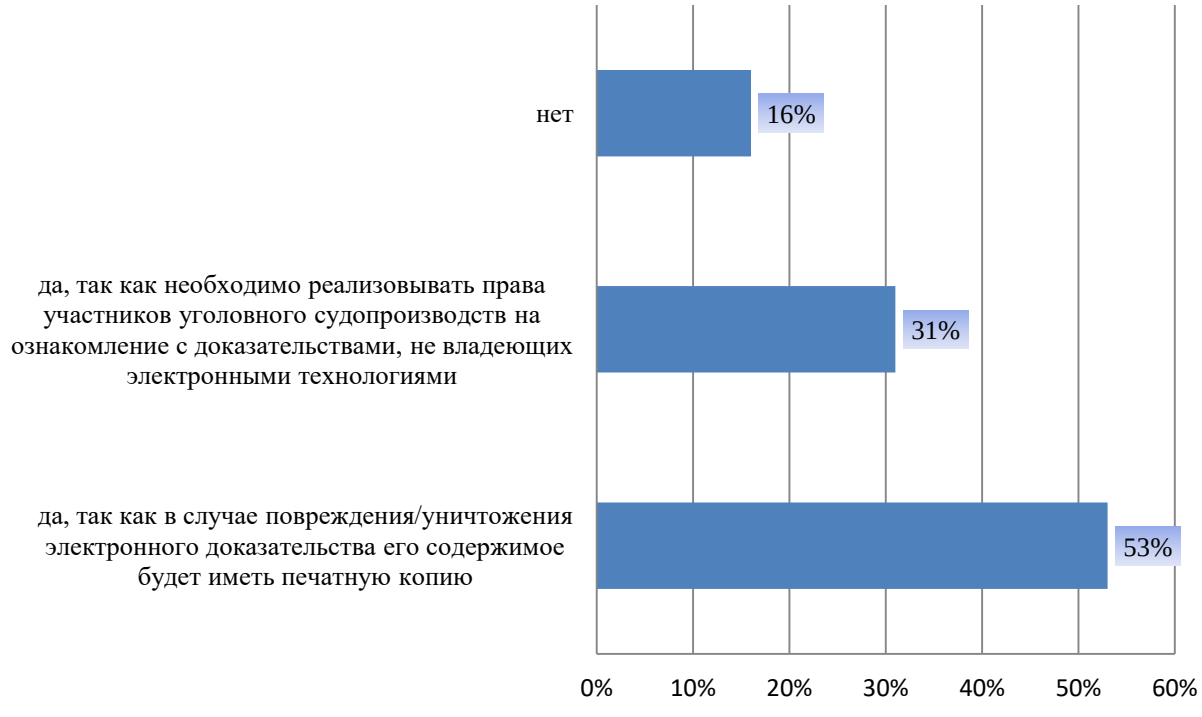
10. По Вашему мнению, какие сомнения возникают у следователя, дознавателя при проверке и оценке электронного доказательства, содержащегося в уголовном деле?



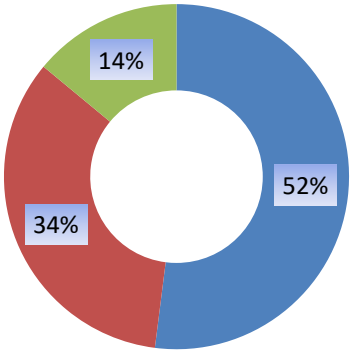
11. Считаете ли Вы необходимым закрепить в ст. 86 УПК РФ способы собирания электронных материалов адвокатом-защитником?



12. Необходимо ли, по Вашему мнению, распечатывать содержание электронного доказательства и приобщать к материалам уголовного дела?



13.Считаете ли Вы, что имеется необходимость в оптимизации уголовно-процессуального законодательства в целях создания правовых условий использования электронных доказательств при исследовании обстоятельств совершенного преступления?



- да, необходимо предусмотреть способы собирания электронных доказательств и их правовое регулирование
- да, так как действующее правовое регулирование не позволяет использовать электронные доказательства в доказывании по уголовным делам исходя из их электронной природы
- нет

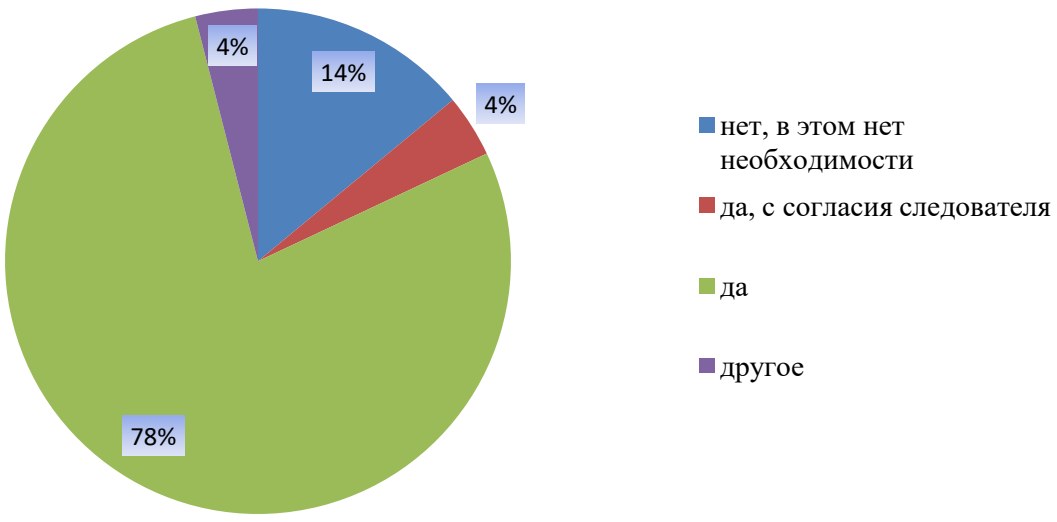
14. По Вашему мнению, необходимо ли определение дополнительных критериев допустимости для электронных доказательств?



15. Какой порядок ознакомления с электронным доказательством в ходе ознакомления с материалами уголовного дела, Вы считаете оптимальным?



16. По Вашему мнению, необходимо ли в УПК РФ предусмотреть дополнительную гарантию прав стороны защиты – возможность приглашать специалиста для ознакомления с материалами уголовного дела в порядке ст. 217 УПК РФ для оказания технической помощи при изучени



Приложение 4.

Действия суда при наличии рисков признания электронных доказательств недопустимыми

Риск	Причина	Действия суда
Несостыковка времени электронного файла с процессуальными событиями	Возможное создание/изменение файла после изъятия, либо неверное системное время, либо подмена источника	Выяснить местонахождение телефона после изъятия, допросить участников, проверить системное время, назначить компьютерно-техническую экспертизу по метаданным
Отсутствие даты/времени на приложениях (фототаблицах, скриншотах)	Суд не может проверить атрибуты без доверия протоколу; снижается воспроизводимость	Исследовать оригинал на устройстве/образ, обеспечить фиксацию метаданных, допросить специалиста, приобщить отчет извлечения данных
Несоответствие визуальной обстановки (сезонность, погодные условия)	Фото может быть не относимым (не то место/не тот период)	Сопоставить фото с осмотром места, ориентиры, при необходимости провести следственный эксперимент/осмотр с фотофиксацией, назначить экспертизу по содержанию изображения (в исключительных случаях)
Неясность происхождения файла (как фото попало в телефон)	Файл может быть получен пересылкой, скачан, автоматически сохранен, подложен	Выяснить расположение файла (папка, приложение), наличие следов пересылки, источники (мессенджер/браузер), назначить экспертизу

		телефона
Отсутствие данных о канале получения сообщения и его содержании	Невозможно установить факт получения координат именно обвиняемым и в нужное время	Исследовать переписку/уведомления, данные приложений, при наличии оснований запросить сведения у операторов/сервисов, оценить непротиворечивость
Разрыв цепочки хранения устройства	Неконтролируемый доступ создает вероятность вмешательства в данные	Проверить по рапортам и показаниям, установить порядок хранения, оценить допустимость и достоверность, при существенных пробелах исключить/обесценить такие сведения
Опора обвинения на единичный цифровой маркер без подтверждения	Повышается вероятность ошибки и предположений	Искать независимые подтверждения (геолокация, логи приложений, объективные записи), оценивать достаточность в совокупности

Приложение 5.

Методические рекомендации
по порядку закрепления следователем, дознавателем
электронных доказательств в ходе предварительного расследования

ОБЩИЕ ПОЛОЖЕНИЯ

В условиях интенсивной цифровизации общественных отношений следователю, дознавателя приходится осматривать значительное количество электронных носителей информации, объем которых может достигать гигабайтов данных. При этом вся получаемая информация фиксируется в протоколах осмотра в письменной форме, что на практике превращается в трудоемкий и малоэффективный способ работы, поскольку следователь, дознаватель фактически вынужден переписывать аналоговым способом уже зафиксированную в цифровой форме информацию. Анализ уголовно-процессуальных требований к составлению протокола следственного действия и приложению к указанному протоколу, научных подходов к закреплению доказательств, а также выявленных проблем уголовно-процессуальной практики в рассматриваемом направлении обуславливает необходимости разработки рекомендаций по закреплению электронных доказательств в уголовном судопроизводстве.

СОДЕРЖАНИЕ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ

1. Закрепление источника и контекста (совокупности сведений об источнике, условиях существования и способе получения электронных данных) происхождения электронных данных.

Обязательным является процессуальное закрепление происхождения сведений, позволяющее установить: где находились данные, каким способом они были получены и как они соотносятся с участниками и обстоятельствами уголовного дела. Для этого в процессуальных документах отражаются тип

источника: устройство, носитель, интернет-ресурс, информационная система, оператор, сервис, его идентификаторы: IMEI/серийный номер для устройства; URL и ID объекта для ресурса; идентификаторы учетной записи или раздела системы, если они доступны и подлежат закреплению в рамках законного доступа, а также условия доступа: включенность/блокировка устройства, наличие авторизации, сетевое подключение, режим получения данных.

2. Индивидуализация электронного носителя и упаковки.

Для исключения сомнений в подмене электронного носителя электронных сведений либо в несанкционированном доступе к ним подлежат обязательному закреплению индивидуализирующие признаки электронного устройства или обозначенного носителя: тип, марка, модель, серийный номер, IMEI, иные идентификаторы, состояние, а также сведения об его упаковке, опечатывании и маркировке. Важным является отражение последующих действий по хранению и передаче электронного носителя или копии. В уголовно-процессуальной практике распространены ситуации, когда в протоколе указываются обобщенные обозначения: телефон, флеш-накопитель, диск, что рождает аргумент о потенциальной заменяемости исследуемого объекта. Подробная индивидуализация и прозрачная цепочка обращения с электронным носителем электронных сведений минимизируют указанную уязвимость.

3. Индивидуализация электронного объекта.

Электронной объект должен быть описан как конкретная единица исследования, а не абстрактная категория: «видеозапись», «аудиофайл», «переписка». Для обеспечения идентифицируемости такого объекта целесообразно фиксировать наименование (при наличии), формат / тип, размер, дату и время (если доступны и значимы), место расположения (путь к файлу, раздел, каталог, объект в приложении), а для аудио- и видеоматериалов – дополнительно длительность, разрешение, иные технические параметры, достаточные для идентификации. Практика показывает, что именно неопределенность относительно того, какой именно файл был получен и

приобщен, формирует значительную часть сомнений о допустимости и доказательственной силе электронных доказательств.

4. Отражение способа получения и объема извлечения электронного файла.

Закрепление электронного доказательства должно обеспечивать его воспроизводимость: необходимо отражать процессуальную форму извлечения рассматриваемого доказательства (посредством осмотра, выемки, обыска, получения сведений от организации, дистанционного осмотра), последовательность существенных действий (осуществление поиска, переходов, открытий разделов, воспроизведения материалов, экспорта, копирования) и объем извлечения (полностью либо выборочно) с указанием критериев отбора. В уголовно-процессуальной практике распространенным основанием для сомнения достоверности электронного доказательства является отсутствие описания того, каким образом осуществлялось копирование или экспорта электронных сведений и какие именно данные включены в копию. Чем более прозрачен и конкретен протокол процессуального действия, тем выше достоверность результата при последующем судебном исследовании.

5. Обеспечение целостности и неизменности электронных данных.

Достоверность электронного доказательства существенно зависит от возможности подтвердить неизменность данных. Поэтому при обращении с электронными носителями следует минимизировать воздействие на исходные данные – исключать запись на оригинал при подключении, избегать действий, изменяющих метаданные, а при копировании обеспечивать контроль целостности электронных данных посредством расчета и закрепления контрольных значений (хэш) файлов или образов, если это технически возможно и соразмерно цели действия. На практике часто сторона защиты указывает, что представленный в уголовном деле объект мог быть пересохранен, перекодирован, смонтирован или заменен, что требует либо проведения дополнительных процессуальных действий, либо оставить под сомнением достоверность полученных электронных сведений. Использование проверяемых механизмов контроля целостности электронных

данных существенно ограничивает основание для подобных возражений стороны защиты и снижает потребность в компенсирующих доказательствах.

6. Документирование и приложение копий электронных данных.

Протокол как текстовый документ должен быть дополнен приложениями, позволяющими повторно проверить содержание и объем полученной информации, носителем электронных данных с копией (или образом), перечнем скопированных объектов с атрибутами, скриншотами и фототаблицами ключевых фрагментов; при необходимости – видеозаписью экрана, демонстрирующей последовательность действий и отображение контента (особенно при закреплении сетевых ресурсов). Практика подтверждает, что при отсутствии перечней и атрибутов, когда к протоколу приложен лишь носитель с файлами, в дальнейшем затрудняется судебная проверка электронного доказательства: возникает неопределенность, что именно являлось предметом осмотра и что конкретно приобщено к материалам уголовного дела.

7. Прослеживаемость хранения и доступа (цепочка хранения) электронных данных.

Закрепление электронных доказательств должно включать элементы, обеспечивающие прослеживаемость обращения с носителем электронных данных и их копиями: место хранения, перечень лиц, имеющих доступ, сведения передаче электронных данных между подразделениями и должностными лицами, состояние упаковки и опечатывания электронного носителя с электронными данными. В правоприменительной практике «разрывы» в цепочке хранения электронных данных являются распространенным аргументом о возможном вмешательстве и подмене электронных данных.

8. Процессуальные решения о признании и приобщении электронных сведений.

После получения и закрепления электронных сведений следователь, дознаватель определяет их процессуальную природу. В зависимости от содержания и характера электронные объекты могут быть признаны вещественными доказательствами в соответствии со ст. 81 УПК РФ

(например, электронные устройства и носители информации, содержащие следы преступления) либо документами по смыслу ст. 84 УПК РФ (например, электронные файлы, переписка, сведения информационных систем). Определение статуса электронных сведений имеет принципиальное значение для дальнейшего обращения с такими объектами в процессе доказывания.

9. Легализация и приобщение электронных сведений к материалам уголовного дела.

Завершающим этапом закрепления электронных доказательств является включение полученных электронных сведений в систему доказательств по уголовному делу. После закрепления результатов следственного действия и определения статуса электронных сведений соответствующий объект признается доказательством и приобщается к материалам уголовного дела. Только после такого процессуального оформления электронные сведения могут быть использованы для установления фактических обстоятельств, и подлежат проверке и оценке в соответствии с требованиями уголовно-процессуального закона.