**Научная статья**
**УДК 343.1:168.3:004.91**
**EDN:** https://elibrary.ru/sgaoks
**DOI:** https://doi.org/10.21202/jdtl.2023.11

# Концепция электронного доказательства в уголовном судопроизводстве

**Анна Александровна Дмитриева** ✉

Южно-Уральский государственный университет (национальный исследовательский университет)
г. Челябинск, Российская Федерация

**Павел Сысоевич Пастухов**

Пермский государственный национальный исследовательский университет
г. Пермь, Российская Федерация;
Пермский институт Федеральной службы исполнения наказаний
г. Пермь, Российская Федерация

## Ключевые слова

Информация,
право,
процесс доказывания,
расследование,
суд,
уголовное дело,
уголовный процесс,
цифровые технологии,
электронное взаимодействие,
электронные доказательства

## Аннотация

**Цель**: раскрытие потенциала цифровой трансформации для выработки оптимальных средств и методов собирания доказательств, внедрения научной организации труда должностных лиц, осуществляющих уголовное судопроизводство. Научный подход концепции состоит в минимизации затрат на собирание доказательственной информации по уголовным делам в электронной форме и электронным способом, а также сохранении материалов уголовного дела в электронной форме.

**Методы**: ведущее место среди методов исследования занимает диалектический метод, в соответствии с которым проблема электронного документа рассматривается во взаимосвязи и взаимозависимости с информационно-технологическим развитием общества. Совокупность методов научного познания в исследовании создает предпосылки для объективного и комплексного подхода к выделенным проблемам.

**Результаты**: авторская концепция электронного доказательства представляет собой систему информационно-технологических и правовых взглядов на уголовно-процессуальную форму, призванную оптимизировать процесс их собирания, фиксации и сохранения в материалах уголовного дела. Развитие концепции нацелено на выработку новых подходов к организации деятельности органов расследования и суда с учетом достижений в сфере информационных технологий, обеспечивающих новые способы собирания уголовно-релевантной,

✉ Контактное лицо

уголовно-процессуальной, криминалистически значимой информации при расследовании и рассмотрении уголовного дела. Представленная концепция направлена также на совершенствование взаимодействия и служебной коммуникации должностных лиц органов предварительного расследования с должностными лицами информационно-технологических систем для собирания доказательственной информации в электронной форме.

**Научная новизна**: системно проанализированы изменения, происходящие в современном информационном обществе через призму возникающих проблем между отраслевым уголовно-процессуальным доказательственным правом и более современными технологическими способами собирания доказательственной информации. В статье демонстрируется новый подход к созданию технологического взаимодействия с использованием цифровых технологий на научной основе организации доказательственной деятельности, призванной оптимизировать и рационализировать процесс доказывания в уголовном судопроизводстве.

**Практическая значимость**: материалы исследования могут быть использованы в работе по подготовке предложений о внесении изменений и дополнений в действующее законодательство с целью реализации практического опыта уже действующих моделей уголовно-процессуальной деятельности зарубежных стран, неисчерпаемого потенциала информационных технологий, программного обеспечения, искусственного интеллекта для рационализации доказывания по уголовным делам.

## Для цитирования

Дмитриева, А. А., Пастухов, П. С. (2023). Концепция электронного доказательства в уголовном судопроизводстве. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

## Содержание

## Введение

Процесс доказывания по уголовным делам является преимущественно мысленной сферой человеческой деятельности, имеет логическое содержание, а поэтому оперирует множественными теоретическими понятиями, но имеющими важное практическое значение. Важнейшее место в совершенствовании уголовно-процессуального доказывания занимает понятие доказательств, так как уголовный процесс представляет собой практическую деятельность по собиранию, проверке и оценке доказательств. Доказательство, как и всякое понятие, имеет содержание и объем, т. е. такую совокупность существенных признаков, отраженных в этом понятии, чтобы обеспечить правоприменителю максимально допустимую свободу в их собирании, проверке и оценке, но в то же время обладать свойствами относимости, допустимости и достоверности. Установление существенных признаков применительно к определению понятия уголовно-процессуального доказательства требует особой осторожности, так как в уголовном процессе на основании доказательств принимаются все решения, в том числе и об ограничении прав и свобод, виновности или невиновности. Поэтому нельзя допустить, чтобы такие важные решения принимались на основе ошибочной или ложной информации.

Осознавая важность существенных признаков для установления ограничительного содержания и объема понятия доказательства как базового элемента процесса доказывания, полагаем, что понятие доказательств должно быть закреплено в законе с учетом изменяющихся условий развития общества. Если цифровая трансформация изменила все базовые устои общества, то право должно соответствовать изменяющимся условиям. Если же право, консервативное по своей природе, не будет меняться в соответствии с трансформацией общества, то у правоприменителя будет возникать все больше проблем.

Произошедшая цифровая трансформация общества, рост киберпреступлений, а поэтому увеличение доказательственного значения цифровых следов преступлений, повсеместное использование де-факто электронных доказательств в практике деятельности правоохранительных органов наталкиваются на проблему отсутствия понятия «электронных доказательств» в уголовно-процессуальном законе. Поэтому ключевая проблема статьи заключается в обосновании необходимости включения понятия «электронное доказательство» в уголовно-процессуальный закон в целях оптимизации процесса доказывания и повышения его эффективности.

Эффективность мы понимаем как соотношение использованных ресурсов и полученных результатов. В информационном обществе гигантский объем электронной информации в современной инфраструктуре создает трудности при работе с информацией для любого человека, но в то же время открывает огромные возможности для органов расследования. В этой связи возникает закономерный вопрос, как добиваться максимального результата при минимуме затрат сил, средств и времени. В этом и заключается концептуальная идея эффективности в соотношении использованных ресурсов и полученных результатов. Авторы статьи нацелены продемонстрировать потенциал информационного общества, раскрыть содержание электронных доказательств в нормативной системе уголовно-процессуальных доказательств и сформулировать концепцию электронного доказательства, а следовательно, более эффективный процесс доказывания. Для достижения поставленной цели в статье

проанализированы тенденции развития электронных доказательств в отдельных системах зарубежных государств.

Исследование проведено в соответствии с диалектическим методом, позволившим авторам рассмотреть проблему электронного документа во взаимосвязи с информационно-технологическим развитием общества.

## 1. Методы и научные подходы к понятию электронных доказательств в российском праве

Продолжающаяся дискуссия среди ученых о понятии, сущности; особенностях собирания, сохранения; проверке электронных доказательств свидетельствует о неоднозначном подходе к названным аспектам. При обсуждении проблемы внедрения электронной доказательственной информации в качестве доказательств в уголовное судопроизводство мы утверждали, что она может быть представлена в классической системе уголовно-процессуальных доказательств. Практика показывает представление электронной доказательственной информации в ином документе, запрашиваемом у субъектов информационно-технологических систем, таких как обладатели информации, системные администраторы, сотрудники служб информационной безопасности, интернет-провайдеры, провайдеры связи, работники банковских и платежных систем, операторы систем видеонаблюдения. Зачастую электронная доказательственная информация представлялась в вещественном доказательстве, а точнее электронных носителях информации, например, смартфонах, планшетах, ноутбуках. После проведения экспертных исследований такая информация приводится в заключении эксперта (специалиста). Мы утверждали, что не следует менять уголовно-процессуальное законодательство с целью включения «электронного доказательства» как нового вида. Мы предлагали расширительное толкование действующего понятия доказательств (Пастухов, 2019). Существующие признаки понятия доказательств в виде «любых сведений», отраженных в ст. 74 Уголовно-процессуального кодекса Российской Федерации (далее – УПК), казалось бы, не делают исключений для какой-либо информации. На расширительное толкование понятия доказательств указывает ст. 84 УПК, предусматривающая закрепление доказательственной информации не только в письменном виде («иные документы»), но и на иных носителях информации, к числу которых можно отнести электронные носители информации.

Мы исходили из того, что относительная новизна электронной информации, несовершенство цифровой инфраструктуры побуждали ученых говорить о новом типе «электронных доказательств» в качестве отдельного самостоятельного уголовно-процессуального источника доказательств. При этом мы полагали, что с адаптацией общества к многочисленным гаджетам и информационным системам опасения относительно электронной информации исчезнут сами по себе. Данный тезис можно проследить на освоении каждым из нас смартфона, компьютеров и их приложений. В настоящее время смартфон в наших руках является банком в кармане, почтовым сервисом, телевизором, а в принципе, рабочим местом. Каждый из нас легко принимает информацию, создает, пересылает, т. е. выполняет все информационные функции. Подтверждением нашему тезису служат государственные и корпоративные тенденции по отказу от бумажных денег, банковских карт, документарных ценных бумаг, трудовых и сберегательных книжек, бумажных медицинских карт и т. д.

Анализируя различные взгляды, выделим сторонников и противников придания самостоятельного статуса электронным доказательствам. Так, В. Г. Голубцов, возражая против признания электронных доказательств, пишет о том, что электронно-цифровые технологии не обладают признаками и сущностными особенностями, влекущими необходимость изменять основные институты процессуального законодательства (Голубцов, 2019).

Отрицая самостоятельное значение электронного доказательства, Л. А. Головко подчеркнул отсутствие новизны (Головко, 2019), полагая, что уголовно-процессуальная категория доказательства гораздо шире и может включать в себя все электронные данные.

За включение электронных доказательств в сферу доказывания выступает М. И. Воронин (Воронин, 2019). По мнению этого автора, в уголовно-процессуальное законодательство следует ввести понятия «электронное доказательство», «электронный документ», «электронный носитель информации». При этом автор предлагает заимствовать понятие «электронный документ» из Федерального закона «Об информации, информационных технологиях и о защите информации»[1]. Основной закон об информационных технологиях определяет электронный документ как документированную информацию, представленную в электронной форме (п. 11.1 ст. 2). От себя выделим ключевой признак электронного документа в законодательном определении – это способность человека его воспринимать с использованием электронных вычислительных машин. Этот признак является ключевым, так как при производстве по уголовным делам человекочитаемость имеет решающее значение при работе со сложной информационно-технологической средой. Помимо этого, следует отметить еще один признак – это возможность передачи электронного документа по информационно-телекоммуникационным сетям или обработки в информационных системах. Данное законодательное определение распространяется на любую электронную информацию, циркулирующую в цифровой среде. Поддерживая включение электронных доказательств, С. В. Зуев считает, что они должны отвечать четким требованиям допустимости, относимости и достоверности (Зуев, Сутягин, 2016).

Принимая во внимание всю полемичность понятия, сущности и перспектив использования электронных доказательств, мы выработали новый подход и сформулировали концепцию, нацеленную на информационно-технологический прорыв в модернизации уголовно-процессуального доказывания и всей уголовно-процессуальной деятельности. Предлагаемая концепция направлена на отрыв от устаревшей (архаичной) документарной (бумажной) технологии фиксации доказательств посредством включения в уголовно-процессуальное законодательство и сопутствующие акты нормативного толкования понятия «электронные доказательства». Данное нововведение разрешит давнюю проблему архаичной документарной формы удостоверения доказательственной информации и позволит применять более совершенные, научно обоснованные способы сохранения доказательственной информации электронным способом при производстве следственных и иных процессуальных действий или изначально запрашивать у обладателей информации, получать и сохранять доказательственную информацию в электронной форме. Сущностным

[1] Об информации, информационных технологиях и о защите информации. № 149-ФЗ (2006). *Собрание законодательства РФ*, *31* (1 ч.), ст. 3448.

элементом предлагаемой концепции является отрыв электронной информации от документарного (бумажного) протокола следователя и электронного носителя информации с перспективой формирования электронного документооборота.

Предлагаемое нами понятие электронных доказательств должно обеспечить преодоление архаичных методов при обращении с электронной доказательственной информацией, внедрить научные методы организации труда, а поэтому важно раскрыть не только их потенциал, но и все современные информационно-технологические конкурентные преимущества электронных способов и электронных форм доказательственной деятельности. Предлагая вышеуказанные нововведения, авторы полагают, что при электронной форме собирания доказательств должны обеспечиваться все необходимые свойства и предъявляемые требования в части их достоверности и допустимости. Ранее мы уже пришли к пониманию необходимости закрепления в уголовно-процессуальном законе понятия «электронных доказательств» в контексте выработки новых подходов к информационному обеспечению уголовно-процессуальной деятельности и предложили включить его в ст. 5 УПК в следующей редакции: «…электронное доказательство – это зафиксированная электронным способом или представленная в электронной форме юридически значимая информация в соответствии с уголовно-процессуальными требованиями, предъявляемыми к доказательствам, в целях установления истины по уголовному делу» (Пастухов, 2022а).

Понятие «данные» также имеет важнейшее значение, так как информационное общество представляет собой «общество данных», где информация кардинально изменяет все условия жизнедеятельности, а скорость обращения информации в цифровой инфраструктуре увеличилась в разы, поэтому возникает настоятельная необходимость предоставить правоприменителю возможности использования электронной информации, электронные данные без жесткой привязки к бумажному или электронному носителю информации. Из сказанного следует, что решение заявленной в статье проблемы мы видим в устранении чрезмерной формализации, упрощении уголовно-процессуальной формы, выработки новых требований допустимости доказательств за счет развития концепции электронных данных и электронных доказательств.

## 1.1. Понятие электронного доказательства в российском уголовно-процессуальном законодательстве

Как ранее уже отмечено нами, российское законодательное определение доказательств как «любых сведений, на основе которых должностные лица, осуществляющие производство, устанавливают обстоятельства, подлежащие доказыванию по уголовному делу», закреплено в ч. 1 ст. 74 УПК РФ[2]. Такое широкое понимание доказательств, казалось бы, легко позволяет органам предварительного расследования и суду использовать доказательственную информацию в любой форме, в том числе электронной.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. (2001). *Собрание законодательства РФ*, *52* (ч. I), ст. 4921.

Между тем, провозглашая свободу собирания доказательственной информации в виде «любых сведений», ч. 2 ст. 74 УПК ограничивает перечень уголовно-процессуальных источников доказательств как средств доказывания семью видами: показаниями подозреваемого, обвиняемого; показаниями потерпевшего, свидетеля; заключением и показанием эксперта; заключением и показаниями специалиста; вещественными доказательствами; протоколами следственных и судебных действий; иными документами. Как можно увидеть, среди перечисленных уголовно-процессуальных средств доказывания нет упоминания об электронных данных, что и представляет собой главную проблему, образующую противоречие между традиционной консервативной следственной моделью и более современными, а поэтому эффективными методами работы с доказательственной информацией. Это противоречие является главной проблемой настоящей статьи. Как уже сказано выше, российская модель уголовного судопроизводства является «следственной», означающей наличие самостоятельной стадии предварительного расследования, связанной с формированием доказательств в письменных материалах уголовного дела. Термин «предварительное» имеет два значения: во-первых, предшествует стадии судебного разбирательства, а во-вторых, выводы органов расследования являются предварительными. Окончательные выводы о виновности или невиновности делаются в суде на основании исследования представленных в материалах уголовного дела доказательствах.

Отмечая в целом важность стадии предварительного расследования, на которой устанавливаются все обстоятельства дела, а в суд направляются только уголовные дела, имеющие реальную судебную перспективу, считаем необходимым отметить недостатки следственной модели, связанные с дефиницией «доказательство». Одним из важных из значимых недостатков российской следственной модели является ее письменный характер, а точнее бумажная форма, что затрудняет эффективное использование электронной доказательственной информации. Следователь формирует все материалы уголовного дела, словно книгу, в протоколах которой подробно описаны получаемые сведения, вместо более современных, малозатратных способов фиксации и сохранения доказательственной информации в электронной форме. Все это происходит потому, что в российской доктрине основным способом фиксации доказательственной информации является описание в протоколе. Все иные способы фиксации считаются факультативными, что вынуждает следователя подробно описывать уже зафиксированное в человекочитаемой форме на различных носителях информации или даже переписывать увиденное, т. е. зафиксированную на видео информацию. Для следователя российский УПК является вроде «инструкции по применению», отклонение от которой влечет нарушение закона или даже недопустимость доказательств. Следственная модель не позволяет ему широко толковать нормы, касающиеся понятия, содержания и объема доказательств. В сложившейся правовой парадигме и уголовно-процессуальной практике любая доказательственная информация, в том числе электронная, должна быть зафиксирована в письменной форме в протоколе следственного действия, в одном из указанных источников (ч. 2 ст. 74 УПК).

Выделенную в статье проблему не решает уголовно-процессуальная норма, предусматривающая собирание доказательств в виде «иных документов» (ч. 2 ст. 84 УПК), в которой говорится, что сведения могут содержаться как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи

и иные носители информации. Проблема не решается названной нормой по причине требований к письменной процессуальной форме доказательства для обеспечения его допустимости. Кроме того, «иные документы» как вид доказательств создаются вне рамок уголовного процесса, а только приобщаются следователем к материалам уголовного дела. Подавляющее же большинство доказательств формируется следователем посредством составления бумажных протоколов в ходе производства следственных действий. Хотя большинство протоколов составляется с помощью компьютерных средств, они все равно должны распечатываться в бумажной форме и прилагаться к материалам уголовного дела.

Включение в 2012 г. в УПК РФ понятия «электронные носители информации», на которых содержится доказательственная цифровая информация (ч. 4 ст. 81, ч. 1 и 4 ст. 81.1, ст. 164.1 УПК РФ), тоже не решает заявленную проблему и не обеспечивает эффективность деятельности. Сложившиеся требования к процессуальной форме обязывают следователя составлять протокол и приобщать к протоколу скопированную на оптический диск доказательственную информацию. Такой подход означает ручной режим работы и дополнительные расходы. Несовершенство ручного режима работы становится более очевидным в информационном обществе, где цифровая инфраструктура автоматически регистрирует огромное количество юридически значимой информации, которая потенциально может быть криминалистически значимой и использоваться в качестве доказательств по уголовным делам. Собирание такой информации в процессе доказывания должно происходить в автоматизированном режиме, но для этого в уголовно-процессуальном законе должно применяться понятие «электронные доказательства». Отсутствие такого понятия побуждает должностных лиц, осуществляющих производство по делу, собирать доказательственную информацию устаревшим, архаичным способом, сохранять ее в бумажных протоколах. Ввиду сохранения такого порядка вышеобозначенное противоречие будет только усугубляться, так как объемы доказательственной информации в цифровой инфраструктуре только растут, а человеческие ресурсы по ее переписыванию ограниченны.

Хотя понятие электронных доказательств можно увидеть в ст. 186.1 УПК, где упоминаются «данные о соединениях», но это частный случай упоминания в законе, который не решает всех проблем. Данные – это факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации[3].

Далее будут раскрыты преимущества введения в уголовный процесс понятий электронных данных и электронных доказательств.

## 2. Результаты концептуального исследования о преимуществах внедрения понятия электронного доказательства

Заявленная концепция электронного доказательства состоит во включении в уголовно-процессуальный закон понятий «электронные данные» и «электронные доказательства» с целью преодоления бумажного способа оформления материалов уголовного дела. Реализация концепции направлена на оптимизацию работы

[3] *ГОСТ Р 50922-2006: Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения*. (2008). Москва: Стандартинформ.

с доказательствами в двух направлениях: во-первых, позволит собирать электронную доказательственную информацию из цифровой инфраструктуры электронным способом; во-вторых, проводить электронным способом следственные и иные процессуальные действия. В обеих ситуациях обеспечивается возможность фиксировать и сохранять полученную доказательственную информацию в электронной форме в материалах уголовного дела. Полагаем, что в результате реализации данной концепции будет обеспечена процессуальная и материальная экономия процесса доказывания по следующим направлениям.

1. Включение этих понятий позволит должностным лицам не только собирать и сохранять в электронной форме доказательственную информацию без привязки и переноса ее на электронном носителе информации, но и фиксировать традиционную аналоговую доказательственную информацию электронным способом, применяя компьютерные, аудио-, видеосредства фиксации. Как известно, собирание доказательств осуществляется двумя основными способами: 1) путем производства следственных действий и составления соответствующих протоколов; 2) путем приобщения доказательственной информации из современной инфраструктуры. В связи с тем, что в настоящее время в банковской, платежной, навигационной системах, сетях сотовой связи, коммуникационных сервисах и мгновенных мессенджерах, информационно-телекоммуникационной сети Интернет, системах видеонаблюдения, огромном количестве интернет-вещей, персональных устройствах пользователей накапливается гигантский объем криминалистически значимой информации, то приобщение электронной доказательственной информации из перечисленных электронных носителей становится приоритетным. Электронный способ изъятия и приобщения электронной доказательственной информации из вышеперечисленных устройств и систем кардинально сократит время по их получению.

2. Получение электронной доказательственной информации в целостном и неизменном виде, а не в виде частичного описания в протоколе следователя, позволит органам расследования получать оригинал, который намного информативнее описания в протоколе. В англосаксонской системе доказательственного права действует правило наилучшего доказательства, согласно которому в любой доказательственной информации первостепенное значение имеет первоисточник (первоначальная форма), содержащий данные о факте. Правило лучшего доказательства, направленного на представление оригинала записи в суд, закреплено в ст. 1002 Федеральных правил доказывания США[4]. Относительно электронных данных утверждается, что к ним применяются обычные требования: надежность способа создания и хранения сообщения данных; надежность способа, которым была проверена целостность сообщения данных; способ, которым был идентифицирован его создатель. Исследование оригинала электронной информации позволяет дополнительно выявить криминалистическое значение метаданных (metadata), позволяющих верифицировать происхождение документа, его автора, изменения электронного документа с момента создания до получения органами расследования[5].

---

4 *Federal Rules of Evidence*. (2020). federal_rules_of_evidence_-_december_2020_0.pdf

5 *Национальный стандарт Российской Федерации: Обеспечение долговременной сохранности электронных документов ГОСТ Р 54989-2012/ISO/TR 18492:2005*. (2013). Москва: Стандартинформ.

3. Получение электронной информации в оригинале снимает противоречия между доказательственной информацией на электронных документах и электронных носителях информации. Данный тезис важен в связи с тем, что в научной литературе продолжается дискуссия в части признания электронной информации в качестве вещественного доказательства (ст. 81, 82 УПК) или иного документа (ст. 84 УПК). Проблема использования электронного документа не решена даже после придания легального статуса электронному документу в судах общей юрисдикции в 2016 г. Федеральным законом от 23 июня 2016 г. № 220-ФЗ в Уголовно-процессуальный кодекс РФ была введена ст. 474.1, устанавливающая порядок использования в уголовном судопроизводстве электронных документов. Сторонам предоставлено право обращаться в суд с ходатайствами, заявлениями, жалобами, представлениями в форме электронного документа, подписанного электронной подписью, посредством заполнения формы, размещенной на официальном сайте суда в сети Интернет. Приказом Судебного департамента возможность использования электронного документа была детализирована в судах общей юрисдикции[6]. Чуть позже, в 2017 г., легальность статуса электронного документа была подтверждена постановлением Пленума Верховного Суда РФ. Согласно вышеуказанным актам нормативного толкования, под электронным документом понимается документ, созданный в электронной форме без предварительного документирования на бумажном носителе, подписанный электронной подписью в порядке, установленном законодательством Российской Федерации[7]. Указанными документами введено понятие «электронный образ документа» (электронная копия документа, изготовленного на бумажном носителе), т. е. переведенная в электронную форму с помощью средств сканирования копия документа, изготовленного на бумажном носителе, заверенная в соответствии с Порядком подачи документов простой электронной подписью или усиленной квалифицированной электронной подписью. Несмотря на разъяснения в вышеуказанных актах нормативного толкования о необходимости использования электронных документов в производстве по уголовным делам, прорыва в цифровизации в уголовном судопроизводстве не произошло.

4. В условиях развития цифровых технологий к настоящему времени разработаны гарантии от модификации электронной доказательственной информации, ее целостности, неизменности, заключающиеся в ее копировании, дублировании, вычислении контрольной суммы; требование ее сохранности как по месту изъятия, так и в ведомственной информационной системе инфраструктуры правоохранительных органов. Одним из самых точных и надежных методов от модификации является вычисление контрольной суммы, т. е. значение хэш-функции (hash value), которая представляет собой битовую строку с выходным результатом хэш-функции[8]. Применение хэш-функций позволяет сжать электронные документы до фиксированного

---

6 Приказ Судебного департамента при Верховном Суде РФ № 251 от 27.12.2016. (2017). *Бюллетень актов по судебной системе*, *2*.

7 Постановление Пленума Верховного Суда РФ № 57 от 26.12.2017 (2017, 29 декабря). *Российская газета*.

8 *ГОСТ Р ИСО/МЭК 27037-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме*. (2014). Москва: Стандартинформ.

числа битов, т. е. вычислить уникальный «дактилоскопический отпечаток» соответствующих документов, который можно использовать для идентификации и неизменности информации[9]. При проверке доказательств сравниваются контрольные числа оригинала и копии электронной доказательственной информации, которые должны совпадать при верификации. Для создания и обеспечения надежного способа получения доказательств в вышеупомянутом стандарте предлагается сохранять электронные данные посредством применения метода, основанного на 128-битном алгоритме хеширования MD5, по своему назначению заменяющему цифровую подпись по отпечатку пальца. Криминалистическое значение алгоритма хеширования заключается в получении фиксированной длины цифровой информации файла вместо произвольной, что является идентифицирующим свойством полученного электронного документа. Дополнительной гарантией использования хэш-функций является сохранение сгенерированного отпечатка в нескольких экземплярах (двух-трех), причем на разных электронных носителях информации и разных устройствах. Например, один экземпляр должен оставаться у обладателя изъятой информации по аналогии с копией протокола обыска, а второй может сохраняться на сервере правоохранительного органа или на цифровой платформе. Названные технические процедуры полностью решат проблемы с идентификацией, изъятой электронной доказательственной информацией.

5. Признание электронного способа фиксации доказательственной информации открывает возможности и перспективы доказывания удаленным способом. Особо остро эта проблема возникла в период пандемии коронавируса, карантина, изоляции. Необходимость осуществления правосудия сделала электронное онлайн-правосудие чуть ли не основным направлением развития российской правовой системы. Элементы дистанционного производства по уголовным делам уже реализуются посредством использования систем видео-конференц-связи. Более того, даже наблюдается процесс расширения технологии видео-конференц-связи на проведение процессуальных действий на стадию предварительного расследования. Вначале видео-конференц-связь применялась только в апелляционном (ч. 2 ст. 389 УПК РФ) и кассационном (ч. 2 ст. 401 УПК РФ) суде, да и то только для участия лиц, содержащихся под стражей. В судах первой инстанции видео-конференц-связь применялась при рассмотрении жалоб в порядке ст. 125 УПК РФ, вопросов, связанных с исполнением приговора (ч. 2 ст. 399 УПК РФ). Наиболее перспективными были положения УПК в части применения видео-конференц-связи, позволявшие допрашивать в суде первой инстанции свидетелей и потерпевших, находящихся в других населенных пунктах (ч. 4 ст. 240 УПК РФ). Самым перспективным решением российского законодателя видится расширение электронного способа при проведении допроса, очной ставки и опознания в ходе предварительного расследования (ст. 189 УПК РФ) с января 2022 г.

6. Придание электронному доказательству легального статуса позволит интегрировать информационные возможности управленческой, административной, информационно-технологической, оперативно-разыскной, технико-криминалистической и уголовно-процессуальной доказательственной деятельности. Интеграция отраслей права и видов правоприменительной деятельности обеспечит кумулятивный

[9] *Национальный стандарт Российской Федерации: Обеспечение долговременной сохранности электронных документов ГОСТ Р 54989-2012/ISO/TR 18492:2005.* (2013). Москва: Стандартинформ.

эффект уголовно-процессуального доказывания. Объединение информационных возможностей видится во внедрении цифровых платформ как наиболее приемлемых комплексных аппаратно-программных решений для обеспечения как межведомственного электронного взаимодействия, так и органов уголовного преследования, всех участников уголовного процесса, стороны защиты и суда. С использованием цифровых платформ формируются новая форма и содержание информационного взаимодействия в автоматизированном режиме, минимизируя медлительность человеческого фактора. Цифровая технология коммуникаций должностных органов предварительного расследования с должностными лицами информационных систем увеличивает скорость обмена информацией, обратную связь между органами и должностными лицами (Зайцев, Пастухов, 2019). Изучение практики деятельности правоохранительных органов показывает тенденции к созданию цифровых платформ: в Министерстве внутренних дел, прокуратуре, адвокатуре, а тем более в корпоративных организациях. Использование цифровых платформ должно трансформировать бумажное делопроизводство в электронный документооборот.

7. Включение понятия «электронное доказательство» открывает перспективы использования искусственного интеллекта, больших данных, видеоаналитики и видеосемантики (Zaytsev et al., 2021; Пастухов, 2022b; Reedy, 2023; Horsman, 2023; Wu & Zheng, 2020; Chen et al., 2020) как наиболее рациональных методов автоматизации при собирании доказательств. Искусственный интеллект вкупе с цифровыми платформами открывает новую эпоху автоматизации и роботизации в доказательственной деятельности по собиранию информации из сетей сотовой связи, навигационных систем, информационных систем и баз данных. Автоматизация исследования всевозможных банков данных намного повысит информационно-аналитические возможности криминалистической регистрации, учетов органов внутренних дел, иных правоохранительных органов, что позволяет обрабатывать большие объемы данных через совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных источников информации, в объемах, которые невозможно обработать вручную за разумное время (Horsman, 2021).

8. Благодаря электронным доказательствам доказывание в перспективе станет процессом идентификации личности (de Hert et al., 2018), информационно-технологических устройств, действий людей, событий, результатов. Для идентификации будут использоваться цифровые способы, основанные на цифровых идентификаторах, цифровом профиле лица (Hoile et al., 2011), цифровых платформах, системе межведомственного электронного взаимодействия, учетов криминалистической регистрации и иных видах автоматической регистрации.

9. Использование Единой системы идентификации и аутентификации, доказавшей свою эффективность за последнее десятилетие, в целях внедрения цифровых платформ для межведомственного взаимодействия правоохранительных органов и судов для идентификации пользователей[10]. К настоящему времени разработана более эффективная система – единая биометрическая система, обеспечивающая обработку, включая сбор и хранение биометрических персональных данных,

[10] Постановление Правительства РФ № 584 от 10.07.2013. (2013). *Собрание законодательства РФ*, *30* (Ч. II), ст. 4108.

их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в целях идентификации и аутентификации физического лица[11]. Единая биометрическая система с использованием информационных технологий наиболее быстро позволяет идентифицировать человека по уникальным физическим признакам, таким как ДНК, лицо, отпечатки пальцев, голос, по подписи, удостоверяющим личность документам (Зайцев, Пастухов, 2022).

10. Использование электронных доказательств открывает перспективы для формирования информационно-технологического режима доказывания, новых стратегий раскрытия и расследования преступлений (Wu & Zheng, 2020). Формирование нового уклада свидетельствует о переходе «от документов к данным», который переводит бумажный документооборот в цифровую форму. В новом цифровом укладе общества перспективной технологией в документообороте является технология блокчейн, которая основывается на принципе контекстовой зависимости. При использовании такой технологии обеспечиваются подлинность, достоверность, неизменность и безопасность электронных документов.

11. На этапе судебного разбирательства в ходе судебного следствия обеспечение проверки электронных доказательств посредством визуализации доказательственной информации с использованием компьютерных, аудио-, видеосредств всеми участниками судебного разбирательства, а не только государственным обвинителем, держащим в руках бумажные материалы уголовного дела. Визуализация оригиналов значительно упрощает демонстрацию технических деталей электронных данных, таких как метаданные, хронология, геолокация, цифровые идентификаторы и другие числовые, временные, навигационные данные на электронных картах.

12. Внедрение электронного документооборота как необходимого условия для процессуальной и материальной экономии как итоговое значение легализации понятия электронного доказательства. Использование понятий электронных данных и электронных доказательств в правовых системах разных государств мира показывает, что бумажные (документарные) материалы уголовного дела стали за последние два десятилетия анахронизмом и атавизмом. Полагаем, что ключевое значение для внедрения электронного документооборота имеет именно использование понятий электронных данных и электронных доказательств в уголовно-процессуальном законодательстве.

Для реализации вышеназванных положений предложенной концепции необходимо проанализировать зарубежное уголовно-процессуальное законодательство.

## 3. Исследование электронного доказательства в правовых системах зарубежных государств

Недопустимо медленные изменения в российском законодательстве и кардинальные изменения в зарубежных правовых системах показали преимущества использования электронных доказательств в уголовно-процессуальных законодательствах для правоприменения, в частности для внедрения электронного документооборота.

[11] Банк России. *Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов*. (2022). https://www.cbr.ru

Анализ понятий электронного доказательства в англосаксонской правовой системе показывает, что цифровые доказательства определяются как информация и данные, которые представляют ценность для расследования и хранятся, принимаются или передаются с помощью электронного устройства[12]. Причем доказательства, полученные из электронных устройств, таких как компьютеры и их периферийные устройства, компьютерных сетей, мобильных телефонов, цифровых камер, устройств хранения данных, а также из Интернета, используются в процессе доказывания на тех же правовых основаниях, что и традиционные формы доказательств (Rogers et al., 2023; Reedy, 2023; Horsman, 2023). Законодательное регулирование электронных доказательств в Великобритании регламентируется Законом о полиции и уголовных доказательствах 1984 г.[13] На все цифровые доказательства распространяются те же правила и законы, которые применяются к документальным доказательствам[14].

Полномочия полиции, закрепленные в ст. 19 Закона полиции, распространяются на истребование любой информации, в том числе в электронной форме. Главное условие заключается в том, чтобы электронная доказательственная информация имела отношение к совершению или предотвращению преступлений, а также когда ее изъятие способствует предотвращению сокрытия, потери, подделки или уничтожения доказательств в любой форме. Аналогичные подходы к цифровым доказательствам изложены в руководстве для полицейских Великобритании[15].

В юридических словарях англосаксонской системы права цифровые доказательства (digital evidence) тоже определяются широко – как информация, имеющая доказательную ценность, хранящаяся или передаваемая в цифровой форме, т. е. любые данные, записанные или сохраненные на любом носителе в компьютерной системе или другом подобном устройстве, которые могут быть прочитаны или восприняты человеком или компьютерной системой[16]. В другом юридическом словаре цифровые доказательства или электронные доказательства понимаются как любая доказательная информация, хранящаяся или передаваемая в цифровом виде, а сторона судебного спора может использовать ее во время судебного разбирательства[17].

В ст. 402 Федеральных правил о доказательствах США цифровые доказательства (digital evidence) и понимаются как данные (data) и носитель, на котором хранятся данные (media storing the data)[18]. Широкое толкование понятия

---

12 National Institute of Justice. (2008, April). *Electronic CSI, a Guide For First Responders, Electronic Crime Scene Investigation*: A Guide for First Responders, Second Edition (ojp.gov).

13 *Police and Criminal Evidence Act 1984*. (1984). https://www.legislation.gov.uk/

14 *Digitally Stored Evidence Standard Operating Procedure. Police Service of Scotland Standard Operating Procedure (SOP)*. (2018). https://www.scotland.police.uk/spa-media/ercbdgot/indecent-images-children-digital-media-sop.pdf

15 *ACPO Good Practice Guide for Digital Evidence*. (2012, March). https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

16 *Lawinsider*. (2021). https://www.lawinsider.org/

17 *US Legal Forms*. (2022). https://uslegal.com/wp-signup.php?new=www.definitions

18 *Federal Rules of Evidence*. (2020). federal_rules_of_evidence_-_december_2020_0.pdf (uscourts.gov)

доказательств и использование в законодательстве понятия «данных» уже давно позволило в США применить электронный документооборот при производстве по уголовным делам. Для реализации этой технологии были разработаны руководства[19], руководящие правила судов всех уровней и регламенты представления документов, технические требования к электронным документам при их копировании, сканировании, к формату, объему, в том числе по использованию электронных автоматизированных банков данных[20]. Размещение материалов уголовного дела в информационно-технологической среде предоставляет участникам уголовного процесса доступ к материалам уголовного дела для ознакомления, уведомления, извещения. Ключевое значение в опубликованных руководствах и практической деятельности по использованию электронного документооборота (Case Management and Electronic Case Files (CM/ECF) system)[21] имеет учетная запись или личный кабинет пользователя. Должностные лица, осуществляющие производство по делу, адвокаты и заявители должны создать учетную запись, в автоматическом режиме получить сгенерированный пароль[22]. За злоупотребление своей учетной записью предусмотрена строгая дисциплинарная и юридическая ответственность.

Введение системы электронного документооборота значительно упрощает судам ведение электронной регистрации и производство дел в электронном виде[23]. Разработанные руководства устанавливают требования к качеству уголовно-процессуальных документов в электронной форме, распределенный доступ сторонам[24].

## 3.1. Понятие электронного доказательства в законодательстве европейских государств

В континентальной системе права на территории Евросоюза расширительное определение электронных доказательств как «любой информации, созданной, сохраненной или переданной в цифровом виде, позволяющей опровергнуть факт, оспариваемый в ходе судебного разбирательства»[25], свидетельствует о наиболее эффективном использовании их при производстве по уголовным делам. Наиболее интенсивная работа в эпоху цифровых технологий по внедрению электронных доказательств в странах Евросоюза началась с принятием в 2018 г. Европейским парламентом Регламента,

---

19 *Electronic case filing administrative policies and procedures manual*. (2020, October). https://www.azd.uscourts.gov/sites/default/files/documents/adm%20manual.pdf

20 *Federal Rules of Evidence. R. 402. 2 Federal Rules of Evidence. R. 803.* (2020). https://www.uscourts.gov/sites/default/files/federal_rules_of_evidence_-_december_2020_0.pdf

21 *Electronic case filing administrative policies and procedures*. https://www.ncmd.uscourts.gov/sites/ncmd/files/ecfprocman.pdf

22 *Electronic case filing (ECF) Manuals and Training*. (2016). http://www.kywd.uscourts.gov/ecf-manuals-and-training

23 *SEC Center for Complaints and Enforcement Tips*. (2021). https://www.sec.gov/whistleblower/submit-a-tip

24 *Enforcement Manual*. (2017, November 28). https://www.sec.gov/divisions/enforce/enforcementmanual.pdf

25 *Electronic evidence guide. A basic guide for police officers, prosecutors and judges. Version 2.1, Strasbourg*. (2020, March). https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf

обеспечивающего механизмы сотрудничества[26]. Расширительное определение электронных доказательств и принятие Регламента наделило правоохранительные и судебные органы современными инструментами по собиранию доказательств в электронной форме и таким образом ускорило процесс их защиты и получения у субъектов информационно-технологических систем, независимо от юрисдикции страны (Horsman, 2023; Hoile et al., 2011; Mason, 2014).

Признание электронных данных в качестве уголовно-процессуального доказательства в странах Евросоюза упрощает взаимодействие при расследовании уголовных дел в разных странах. В целях развития правовой помощи по уголовным делам и оперативного сохранения доказательственной информации Европарламентом принят Регламент, устанавливающий обязательные европейские ордера на сохранение электронных данных (European Preservation Order). По установленной процедуре выдается приказ, который утверждается судебным органом запрашивающей страны. За непредоставление запрашиваемой информации предусмотрена жесткая административная ответственность в виде штрафов. Наряду с ордерами о сохранении информации Европарламентом принят Европейский ордер о предоставлении (European Production Order). Исполнителями ордеров признаны обладатели цифровой доказательственной информации в информационно-телекоммуникационных сетях, такие как интернет-провайдеры, провайдеры связи, системные администраторы, так называемые поставщики услуг электронной связи.

## 3.2. Понятие электронных доказательств в Китайской Народной Республике

Созданный в Китайской Народной Республике (далее – КНР) информационно-технологический потенциал создает базис для собирания электронной доказательственной информации, обеспечивая новый информационно-технологический режим доказывания. Цифровое развитие в Китае в корне изменяет информационно-аналитическое и информационно-технологическое обеспечение расследования преступлений. Произошедшие в КНР изменения позволили перейти от документов к данным с одновременным упрощением процессуальной формы уголовного судопроизводства. Новые подходы позволили, по существу, ликвидировать документарный (письменный) характер производства по делу и перейти на электронный формат уголовного дела.

Эпоха электронных доказательств началась с принятием поправок УПК КНР в 2012 г. К существующим устным доказательствам: заявлениям потерпевших, показаниям свидетелей, показаниям и объяснениям подозреваемых и обвиняемых в совершении преступления; вещественным и письменным доказательствам; заключениям эксперта; протоколам осмотра и освидетельствования; видео- и аудиоматериалам – были добавлены электронные данные[27]. Таким образом, УПК КНР

[26] *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*. (2018). https://www.eclan.eu/en/eu-legislatory/proposal-for-a-regulation-of-the-european-parliament-and-of-the-council-on-european-production-and-preservation-orders-for-electronic-evidence-in-criminal-matters-e-evidence

[27] *Уголовно-процессуальный кодекс КНР.* (2012). https://asia-business.ru/law/law1/criminal/procedurallaw/

с 2012 г. «электронные данные» признаются доказательствами, хотя уголовно-процессуальный закон не раскрывал это понятие (Юншен, 2014).

В развитие уголовно-процессуального закона в КНР разработано совместное Положение «О решении некоторых вопросов, касающихся собирания, получения и анализа электронных данных по уголовным делам», в котором закреплено понятие электронных данных. В ст. 1 названного положения ««электронные данные» определяются как информация, собранная в рамках уголовного дела, сохраненная и передаваемая в электронной форме, которая может служить доказательством по уголовному делу»[28].

В ст. 2 положения дана классификация электронных данных, признаваемых доказательствами по уголовному делу, среди которых: веб-сайты, блоги (онлайн-дневники), микроблоги, страницы в социальных сетях, идентификаторы приложения (например, WeChat), форумы, онлайн-диски (онлайновые хранилища). Самое многочисленное значение имеют коммуникации в сети Интернет и сетях связи, например, мобильных сообщениях, электронных письмах, сообщениях из мессенджеров, сообщениях в группах. Особо важное значение имеет идентификационная информация, полученная при регистрации пользователя на сайте, электронных транзакциях, журналах регистрации.

С включением электронных доказательств в уголовно-процессуальное законодательство некоторые ученые оптимистично отмечали, что в эру электронных доказательств произойдет исторический скачок в теории доказательств (Guo, 2023; Wu & Zheng, 2020; Chen et al., 2020).

В целях обеспечения гарантий целостности и неизменности при собирании электронных доказательств в ст. 7 Положения предписывается производить их извлечение одновременно двумя следователями. В Положении указывается на строгое соблюдение всех перечисленных технических стандартов и юридических требований под угрозой их недопустимости, указанных в уголовно-процессуальном законодательстве.

Так, при изъятии исходный носитель данных опечатывается и производится стенограмма состояния хранения первоначального носителя. Опечатка оригинального носителя электронных данных и его фотосъемка должны защитить информацию от редактирования. В случае невозможности изъятия исходного носителя и находящихся в нем электронных данных производится стенограмма с указанием причин невозможности изъятия, источника электронных данных и места его хранения. Электронные данные, находящиеся вне территории КНР, могут быть извлечены через Интернет. По окончании расследования уголовного дела оригинальный носитель или собранные электронные данные должны быть переданы вместе с делом в опечатанном виде. Кроме того, в народную прокуратуру и суд передаются резервные копии (Юань, 2017).

При проверке электронных данных в прокуратуре и суде подлежат анализу, изучению законность их получения, подлинность и действительность (актуальность).

---

[28] Положение Верховного народного суда КНР, Верховной народной прокуратуры КНР и Министерства общественной безопасности КНР. (2016). https://splcgk.court.gov.cn/gzfwww//spyw/spywDetails?id=84ba1d7cbc0540d59fe49341f8b1ef85

Во всех юрисдикциях возникают проблемы с хранением электронных данных в органах расследования и передачи материалов дела в суд. Во всем мире разрабатываются цифровые платформы, создаются базы данных, используются межведомственные информационные сети. В этом плане в КНР создали интегрированную базу данных, основанную на технологии онлайн-хранилища (по типу iCloud) для фиксации, хранения и передачи материалов уголовных дел в электронной форме в суд. Основными функциями облачного хранилища китайских правоприменителей являются не только хранение и архивирование, но и быстрый поиск нужных материалов в больших массивах электронных данных. Разработчики данной информационной платформы предусмотрели функции по надзору за всеми стадиями уголовно-процессуальной деятельности, от надзора за предварительным расследованием до стадий по пересмотру вышестоящими инстанциями.

Итак, анализ китайского уголовно-процессуального законодательства в части закрепления электронных данных в качестве доказательств в КНР свидетельствует о модернизации китайского уголовного процесса.

### 3.3. Выработка международных стандартов к электронным доказательствам

Во всех междугородных документах по киберпреступности отмечается, что цифровые данные являются основой большинства расследований преступлений и предпринимаются усилия по дополнительному правовому регулированию. В Европейской конвенции по киберпреступности компьютерные данные означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию (п. б ст. 1) [29].

В Конвенции «данные о потоках» определяются как любые компьютерные данные, относящиеся к передаче информации посредством компьютерной системы, которые генерируются компьютерной системой, являющейся составной частью соответствующей коммуникационной цепочки, и указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса (п. д ст. 1). Понятиями «данные» Конвенция оперирует при оперативном обеспечении и сохранности, обыске и выемке хранимых компьютерных данных. Самые перспективные положения были заложены в ст. 20 Конвенции, предусматривающей сбор в режиме реального времени данных о потоках информации. В частности, на государства возлагались обязанности по принятию законодательных и иных мер, необходимых для предоставления компетентным органам полномочий по собиранию или записыванию с применением технических средств в реальном режиме времени данных о потоках информации и в рамках правового сотрудничества передаче данных заинтересованной стороне.

Международная организация уголовной полиции, более известная как Интерпол, является организацией, содействующей полицейскому сотрудничеству между

[29] *Конвенция о преступности в сфере компьютерной информации (ETS № 85)*. https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#OB9knUTgvfe6Gfbu1

странами-членами. В правилах Интерпола по обмену информацией «данные» означают любую информацию, независимо от ее источника, относящуюся к составляющим элементам общеуголовных преступлений, расследованию и предотвращению таких преступлений, уголовному преследованию правонарушителей и наказанию за них[30]. В принятом в Интерполе руководстве по обращению с электронными доказательствами при проведении обыска и выемки, их идентификации с помощью методов, гарантирующих их целостность, рекомендуется обращаться с ними, как и со всеми другими традиционными доказательствами. Необходимо учитывать, что некоторые электронные устройства требуют особых процедур сбора, упаковки и транспортировки либо потому, что они подвержены повреждению электромагнитными полями, либо потому, что их содержимое может измениться во время обращения и резервирования[31].

Российский стандарт по информационным технологиям, методам обеспечения безопасности, выявлению и раскрытию электронной информации вводит новое понятие «электронное раскрытие» (electronic discovery), которое служит движущей силой как при проведении расследований, так и в ходе работы по сбору и обработке доказательств[32]. Электронное раскрытие (э-раскрытие) представляет собой процесс выявления и представления соответствующей сохраняемой в электронном виде информации (Electronically Stored Information, ESI) или данных одной или несколькими сторонами, участвующими в расследовании или судебном разбирательстве либо в аналогичных процедурах. Составными элементами э-раскрытия стандарт предусматривает сбор, обеспечение сохранности, представление, передачу сохраняемой в электронном виде информации. Это один из современных стандартов, основанный на более ранних стандартах, которые также рассматривали свидетельства, представленные в цифровой форме (digital evidence). В этом стандарте говорится, что информацию или данные, хранящиеся или передаваемые в виде двоичного кода, можно использовать в качестве доказательства[33].

## Выводы

Завершая исследование, отметим, что авторская концепция электронного доказательства представляет собой систему информационно-технологических и правовых взглядов на уголовно-процессуальную форму, призванную оптимизировать процесс их собирания, фиксации и сохранения в материалах уголовного дела. Основная цель

---

30 *Interpol's Rules on the Processing of Data*. (2021, March). https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

31 *Guidelines for digital forensics first responder. Best practices for search and seizure of electronic and digital evidence*. (2021). https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

32 *ГОСТ Р ИСО/МЭК 27050-1-2019 Информационные технологии. Методы обеспечения безопасности. Выявление и раскрытие электронной информации. Часть 1. Обзор и концепции*. (2019). Москва: Стандартинформ.

33 *ИСО/МЭК 27037:2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме» (ISO/IEC 27037:2014 «Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence»)*. (2014).

заявленной концепции состоит в модернизации уголовно-процессуального доказывания при раскрытии потенциала электронных доказательств по вышеназванным направлениям.

Реализация заявленной концепции позволит совершить прорыв в архаичной системе доказательственного права и уйти от письменной (бумажной) формы фиксации доказательств. Первым шагом для реализации названной концепции должно стать включение в УПК понятия «электронные доказательства», что повлечет за собой свободное оперирование органами расследования и судом электронной доказательственной информацией и использовать ее в качестве средств доказывания. Сущностным элементом предлагаемой концепции является отрыв электронной информации от документарного (бумажного) протокола следователя и электронного носителя информации с перспективой формирования электронного документооборота в межведомственной цифровой платформе.

Предложенное нами ранее понятие об электронных доказательствах в контексте выработки новых подходов к информационному обеспечению уголовно-процессуальной деятельности мы предлагаем рассматривать в рамках более широкой концепции и включить в ст. 5 УПК в следующей редакции: «…электронное доказательство – это зафиксированная электронным способом или представленная в электронной форме юридически значимая информация в соответствии с уголовно-процессуальными требованиями, предъявляемыми к доказательствам, в целях установления истины по уголовному делу» (Пастухов, 2022а).

Наряду с введением понятия «электронные доказательства», в ст. 84 УПК необходимо включить понятие «электронные данные», предназначенные для слома устаревшей системы документарных «иных документов».

В условиях информационного общества, развитой цифровой инфраструктуры включение этих понятий позволит создать информационно-технологический режим доказывания на научной основе организации труда. Говоря практическим языком, это позволит по-новому обеспечить информационное преимущество органов расследования и судов перед криминальной деятельностью в части собирания и фиксации электронной доказательственной информации. В части взаимодействия органов предварительного расследования с любыми субъектами информационно-технологических систем позволит кардинально сократить временные, процессуальные, материальные издержки посредством электронного документооборота. Включение этого понятия позволит должностным лицам не только собирать и сохранять в электронной форме доказательственную информацию без привязки и переноса ее на электронном носителе информации, но и фиксировать традиционную аналоговую доказательственную информацию электронным способом, применяя компьютерные, аудио-, видеосредства фиксации.

## Список литературы

Воронин, М. И. (2019). Электронные доказательства в УПК: быть или не быть? *Lex russica*, *7*, 74–84 EDN: https://elibrary.ru/jzbdut. DOI: https://doi.org/10.17803/1729-5920.2019.152.7.074-084

Головко, Л. В. (2019). Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? *Вестник экономической безопасности*, *1*, 15–25. EDN: https://elibrary.ru/korqgw. DOI: https://doi.org/10.24411/2414-3995-2019-10002

Голубцов, В. Г. (2019). Теория доказательств и цифровизация в гражданском судопроизводстве. *Пермский юридический альманах. Ежегодный научный журнал*, *1*, 379–387. https://elibrary.ru/zywect

Зайцев, О. А., Пастухов, П. С. (2019). Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации. *Вестник Пермского университета. Юридические науки*, *46*, 752–777. https://doi.org/10.17072/1995-4190-2019-46-752-775

Зайцев, О. А., Пастухов, П. С. (2022). Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений. *Вестник Пермского университета. Юридические науки, 56*, 281–308. https://doi.org/10.17072/1995-4190-2022-56-281-309

Зуев, С. В., Сутягин, К. И. (2016). *Уголовный процесс*: учебник. Челябинск: Издательский центр ЮУрГУ.

Пастухов, П. С. (2019). Электронные доказательства в нормативной системе уголовно-процессуальных доказательств. *Пермский юридический альманах*, *2*, 695–707. https://elibrary.ru/htypyz

Пастухов, П. С. (2022a). Новые подходы к информационному обеспечению уголовно-процессуальной деятельности. В сб. Т. В. Евтух, Л. Ю. Мхитарян и др. (ред. кол.), А. Н. Самойлов (отв. ред.), С. А. Котова (отв. за вып.), *Государственное и муниципальное управление в России: состояние, проблемы и перспективы: материалы Всерос. науч.-практ. конф., г. Пермь, 17 ноября 2022 г.* (с. 139–143). Пермь: Перм. филиал РАНХиГС.

Пастухов, П. С. (2022b). Цифровая идентификация личности. В книге: Т. П. Подшивалов, Е. В. Титова, Е. А. Громова (ред.). *Право цифровой среды*: монография (с. 625–632). Москва: Проспект. https://elibrary.ru/zomcik

Юань, И. (2017). Проблемы рассмотрения доказательств по новому УПК КНР. *Социально-политические науки*, *3*, 137–138.

Юншэн, Ч. (2014). Законодательные правила использования электронных данных результатов обыска и ареста. *Современное право*, *36*(5), 111–113.

Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. (2020). Study and implementation on the application of blockchain in electronic evidence generation. *Forensic Science International: Digital Investigation*, *35*, 301001. https://doi.org/10.1016/j.fsidi.2020.301001

de Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Computer Law & Amp; Security Review*, *34*(2), 327–336. https://doi.org/10.1016/j.clsr.2018.01.003

Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Amp; Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Hoile, R., Banos, C., Colella, M., & Roux, C. (2011). Bioterrorism: The effects of biological decontamination on the recovery of electronic evidence. *Forensic Science International*, *209*(1–3), 143–148. https://doi.org/10.1016/j.forsciint.2011.01.017

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Amp; Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & Amp; Justice*, *63*(1), 116–126. https://doi.org/10.1016/j.scijus.2022.11.004

Lippman, M. R. (2019). *Criminal Procedure*. Sage.

Mason, S. (2014). Electronic evidence: A proposal to reform the presumption of reliability and hearsay. *Computer Law & Amp; Security Review*, *30*(1), 80–84. https://doi.org/10.1016/j.clsr.2013.12.005

Reedy, P. (2023). Digital Evidence: Overview. *Encyclopedia of Forensic Sciences* (3rd ed., pp. 21–24). https://doi.org/10.1016/b978-0-12-823677-2.00268-3

Rogers, M., Piper, M., & Bates, S. (2023). A Brief History of Digital Forensics and Digital Evidence. In *Encyclopedia of Forensic Sciences* (3rd ed., pp. 9–18). https://doi.org/10.1016/b978-0-12-823677-2.00029-5

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Amp; Security Review*, *42*, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Amp; Security Review, 36*, 105401. https://doi.org/10.1016/j.clsr.2020.105401

Zaytsev, O. A., Pastukhov, P. S., Fadeeva, M. Y., & Perekrestov, V. N. (2021). Artificial Intelligence as a New IT Means of Solving and Investigating Crimes. *Lecture Notes in Networks and Systems*, *155*, 1266–1273. https://doi.org/10.1007/978-3-030-59126-7_138

## Сведения об авторах

**Дмитриева Анна Александровна** – доктор юридических наук, доцент, заведующий кафедрой уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет (национальный исследовательский университет)
**Адрес:** 454080, Российская Федерация, г. Челябинск, проспект Ленина, 76
**E-mail:** annadm@bk.ru
**ORCID ID:** https://orcid.org/0000-0002-1035-1387
**Web of Science Researcher ID**:
https://www.webofscience.com/wos/author/record/GWU-5850-2022
**Scopus Author ID:** https://www.scopus.com/authid/detail.uri?authorId=57281194100
**Google Scholar ID**: https://scholar.google.com/citations?user=B0PWOwEAAAAJ
**РИНЦ Author ID**: https://www.elibrary.ru/author_items.asp?authorid=312402

**Пастухов Павел Сысоевич** – доктор юридических наук, доцент, профессор кафедры уголовного процесса и криминалистики, Пермский государственный национальный исследовательский университет; профессор кафедры публичного права, Пермский институт Федеральной службы исполнения наказаний
**Адрес:** 614990, Российская Федерация, г. Пермь, ул. Букирева, 15;
614012, Российская Федерация, г. Пермь, ул. Карпинского, 125
**E-mail:** pps64@mail.ru
**ORCID ID:** https://orcid.org/0000-0003-0391-5540
**Web of Science Researcher ID**:
https://www.webofscience.com/wos/author/record/B-5451-2017
**Scopus Author ID:** https://www.scopus.com/authid/detail.uri?authorId=56926673600
**Google Scholar ID**: https://scholar.google.com/citations?user=fu844_kAAAAJ
**РИНЦ Author ID**: https://www.elibrary.ru/author_items.asp?authorid=405105

## Вклад авторов

Обоснование концепции исследования; проведение сравнительного анализа; обобщение результатов исследования; формулировка выводов; интерпретация результатов исследования осуществлялись А. А. Дмитриевой и П. С. Пастуховым в равных долях.

## Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

## Финансирование

Исследование не имело спонсорской поддержки.

## История статьи

Дата поступления – 5 января 2023 г.
Дата одобрения после рецензирования – 5 февраля 2023 г.
Дата принятия к опубликованию – 6 марта 2023 г.
Дата онлайн-размещения – 10 марта 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.11

# Concept of Electronic Evidence in Criminal Legal Procedure

**Anna A. Dmitrieva** ✉

South Ural State University (National Research University)
Chelyabinsk, Russian Federation

**Pavel S. Pastukhov**

Perm State National Research University
Perm, Russian Federation;
Perm Institute of the Federal Penitentiary Service
Perm, Russian Federation

## Keywords

Court,
criminal case,
criminal procedure,
digital technologies,
electronic evidences,
electronic interaction,
Information,
investigation,
law,
proving process

## Abstract

**Objective**: elucidating the potential of digital transformation for elaborating the optimal means and methods of collecting evidences and introducing scientific organization of labor of the officials implementing criminal procedure. The scientific approach within the concept consists in minimizing the costs of collecting evidentiary information in criminal cases in electronic form and by electronic means, as well as storing the criminal case materials in electronic form.

**Methods**: dialectic method occupies the leading position among the research methods, the issues of electronic documentation being considered in the interaction and interdependence with information-technological development of the society. The set of scientific cognition methods within the research creates prerequisites for objective and comprehensive approach to the problems under study.

**Results**: the authors' concept of electronic evidence is a system of information-technological and legal views on the criminal-procedural form, which is intended for optimizing the process of collecting, registering and preserving them in the criminal case materials. The concept development is aimed at elaborating new approaches to organizing the work of investigation agencies and courts, taking into account the achievements in the sphere of information technologies, providing new techniques of collecting criminal-relevant, criminal-procedural, criminological significant information when investigating and hearing of a criminal case. The proposed concept is also aimed at improving interaction and in-service communication of the officials of the preliminary

✉ Corresponding author

investigation bodies with the officials of information-technological systems for the purposes of collecting evidentiary information in electronic form.

**Scientific novelty**: the changes were systemically analyzed, which are taking place in the contemporary information society, through the prism of the emerging problems between the sectoral criminal-procedural evidentiary law and more modern technological means of collecting evidentiary information. The article demonstrates a new approach to creating technological interaction using digital technologies, on the scientific base of organization of proving activity, intended to optimize and rationalize the process of proving in criminal procedure.

**Practical significance**: the research materials can be used to prepare proposals on making changes and additions in the current legislation with a view of implementing the practice of already functioning models of criminal-procedural activity of foreign countries, an inexhaustible potential of information-technologies, software, and artificial intelligence to rationalize proving in criminal cases.

## For citation

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

## References

Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. (2020). Study and implementation on the application of blockchain in electronic evidence generation. *Forensic Science International: Digital Investigation*, *35*, 301001. https://doi.org/10.1016/j.fsidi.2020.301001

de Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Computer Law & Amp; Security Review*, *34*(2), 327–336. https://doi.org/10.1016/j.clsr.2018.01.003

Golovko, L. V. (2019). The digitalization in criminal procedure: local optimization or global revolution? *Vestnik ekonomicheskoi bezopasnosti*, *1*, 15–25. (In Russ.). https://doi.org/10.24411/2414-3995-2019-10002

Golubtsov, V. G. (2019). Theory of evidence and digitization in civil proceedings. *Perm Legal Almanac*, *1*, 379–387. (In Russ.).

Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Amp; Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Hoile, R., Banos, C., Colella, M., & Roux, C. (2011). Bioterrorism: The effects of biological decontamination on the recovery of electronic evidence. *Forensic Science International*, *209*(1–3), 143–148. https://doi.org/10.1016/j.forsciint.2011.01.017

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Amp; Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & Amp; Justice*, *63*(1), 116–126. https://doi.org/10.1016/j.scijus.2022.11.004

Lippman, M. R. (2019). *Criminal Procedure*. Sage.

Mason, S. (2014). Electronic evidence: A proposal to reform the presumption of reliability and hearsay. *Computer Law & Amp; Security Review*, *30*(1), 80–84. https://doi.org/10.1016/j.clsr.2013.12.005

Pastukhov, P. S. (2019). Electronic evidence in the regulatory system of criminal procedural evidence. *Perm Legal Almanac*, *2*, 695–707. (In Russ.).

Pastukhov, P. S. (2022a). New approaches to information provision of criminal-procedural activity. In: T. V. Evtukh, L. Yu. Mkhitaryan et al. (Ed. board), A. N. Samoilov (xec. ed.), S. A. Kotova (in charge of the issue), *State and municipal governance in Russia: condition, problems and prospects: works of the All-Russia scientific-practical conference, Perm, November 17, 2022* (pp. 139–143). Perm: Perm. filial RANKhIGS. (In Russ.).

Pastukhov, P. S. (2022b). Digital identification of a personality. In T. P. Podshivalov, E. V. Titova, E. A. Gromova (Eds.), *Digital environment law* (pp. 625–632). Moscow: Prospekt. (In Russ.).

Reedy, P. (2023). Digital Evidence: Overview. *Encyclopedia of Forensic Sciences* (3rd ed., pp. 21–24). https://doi.org/10.1016/b978-0-12-823677-2.00268-3

Rogers, M., Piper, M., & Bates, S. (2023). A Brief History of Digital Forensics and Digital Evidence. *Encyclopedia of Forensic Sciences* (3rd ed., pp. 9–18). https://doi.org/10.1016/b978-0-12-823677-2.00029-5

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Amp; Security Review*, *42*, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Voronin, M. I. (2019). Electronic Evidence in the Criminal Procedure Code: To Be or not to Be? *Lex Russica*, *7*, 74–84. (In Russ.). https://doi.org/10.17803/1729-5920.2019.152.7.074-084

Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Amp; Security Review, 36*, 105401. https://doi.org/10.1016/j.clsr.2020.105401

Yuan, Yi. (2017). Study on judge's capacity on evidence review from the perspective of the revised criminal procedure law of China. *Sociopolitical Sciences*, *3*, 137–138. (In Russ.).

Yunshehn, Ch. (2014). Legislative rules of using electronic data on the results of search and arrest. *Sovremennoe Pravo*, *36*(5), 111–113. (In Russ.).

Zaytsev, O. A., & Pastukhov, P. S. (2019). Formation of a New Strategy for Crime Investigation in the Era of Digital Transformation. *Vestnik Permskogo Universiteta. Yuridicheskie Nauki*, *46*, 752–777. (In Russ.). https://doi.org/10.17072/1995-4190-2019-46-752-775

Zaytsev, O. A., & Pastukhov, P. S. (2022). Digital personal profile as an element of the information and technological strategy of crime investigation. *Vestnik Permskogo Universiteta. Yuridicheskie Nauki*, *56*, 281–308. (In Russ.). https://doi.org/10.17072/1995-4190-2022-56-281-309

Zaytsev, O. A., Pastukhov, P. S., Fadeeva, M. Y., & Perekrestov, V. N. (2021). Artificial Intelligence as a New IT Means of Solving and Investigating Crimes. *Lecture Notes in Networks and Systems*, *155*, 1266–1273. https://doi.org/10.1007/978-3-030-59126-7_138

Zuev, S. V., & Sutyagin, K. I. (2016). *Criminal procedure*: tutorial. Chelyabinsk: Izdatel'skii tsentr YUURGU. (In Russ.).

## Authors information

**Anna A. Dmitrieva** – Doctor of Law, Associate Professor, Head of the Department of Criminal and Penal Law and Criminology, South Ural State University (National Research University)
**Address:** 76 prospekt Lenina, 454080 Chelyabinsk, Russian Federation
**E-mail:** annadm@bk.ru
**ORCID ID:** https://orcid.org/0000-0002-1035-1387
**Web of Science Researcher ID**:
https://www.webofscience.com/wos/author/record/GWU-5850-2022
**Scopus Author ID:**
https://www.scopus.com/authid/detail.uri?authorId=57281194100
**Google Scholar ID**: https://scholar.google.com/citations?user=B0PWOwEAAAAJ
**RSCI Author ID**: https://www.elibrary.ru/author_items.asp?authorid=312402

**Pavel S. Pastukhov** – Doctor of Law, Associate Professor, Professor of the Department of Criminal Procedure and Criminology, Perm State National Research University; Professor of the Department of Public Law, Perm Institute of the Federal Penitentiary Service
**Address:** 15 Bukirev Str., 614990 Perm, Russian Federation; 125 Karpinskiy Str., 614012 Perm, Russian Federation
**E-mail:** pps64@mail.ru
**ORCID ID:** https://orcid.org/0000-0003-0391-5540
**Web of Science Researcher ID**:
https://www.webofscience.com/wos/author/record/B-5451-2017
**Scopus Author ID:** https://www.scopus.com/authid/detail.uri?authorId=56926673600
**Google Scholar ID**: https://scholar.google.com/citations?user=fu844_kAAAAJ
**RSCI Author ID**: https://www.elibrary.ru/author_items.asp?authorid=405105

## Authors' contributions

Substantiation of the research concept; comparative analysis; summarization of the research results; wording of conclusions; interpretation of the research results were carried out by A. A. Dmitrieva and P. S. Pastukhov in equal parts.

## Conflict of interests

The authors declare no conflict of interests.

## Funding

The research was not sponsored.

## Article history

Date of receipt – January 5, 2023
Date of approval – February 5, 2023
Date of acceptance – March 6, 2023
Date of online placement – March 10, 2023