МРНТИ 20.51.23
УДК 10.19 **DOI 10.70239/arsu.2025.t80.n2.07**

ЦИФРОВЫЕ ДАННЫЕ И СЛЕДЫ В ЭЛЕКТРОННОЙ СРЕДЕ — ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВ В БОЛГАРСКОМ СУДЕ

БАНКОВА Д.*, ДИМИТРОВ В.

***Банкова Добромира** – докторант, Софийский университет «Св. Климент Охридский», г. София, Болгария
E-mail: bankovagan@fmi.uni-sofia.bg, https://orcid.org/0000-0002-9261-2842
Димитров Владимир – профессор, Софийский университет «Св. Климент Охридский», г. София, Болгария
E-mail: cht@fmi.uni-sofia.bg, https://orcid.org/0000-0002-7441-253X

Аннотация. Цифровизация современного общества значительно изменила способ взаимодействия между участниками правоотношений, включая способы формирования, передачи и хранения юридически значимой информации. Возрастающая роль цифровых технологий и электронных коммуникаций обусловливает необходимость переосмысления традиционных правовых подходов к сбору, проверке и оценке доказательств, особенно в судебных разбирательствах.

В Болгарии на протяжении последних лет были приняты существенные изменения в процессуальном законодательстве, направленные на адаптацию правовой системы к условиям цифровой среды. Тем не менее, несмотря на наличие общей нормативной базы, в правоприменительной практике сохраняются значительные пробелы, особенно в отношении оценки цифровых следов, метаданных, данных с временной чувствительностью (например, оперативной памяти) и других нестандартных электронных носителей информации. Проблематика заключается не только в технической способности извлечь и сохранить такие данные, но и в юридической интерпретации их доказательственной силы в контексте установления объективной истины.Цель настоящего исследования — проанализировать возможности применения цифровых данных в качестве доказательств в болгарском судопроизводстве, выявить существующие нормативные и практические барьеры, а также предложить методологию, обеспечивающую юридическую допустимость, достоверность и воспроизводимость электронных доказательств. В рамках данной работы предпринимается попытка интеграции международных технических стандартов и принципов судебной экспертизы с национальной правовой практикой, что позволит создать основу для дальнейшей унификации и стандартизации работы с цифровыми доказательствами в болгарском правосудии.

Ключевые слова: цифровые данные, электронные доказательства, судебное разбирательство, метаданные, целостность данных, квалифицированная электронная подпись.

Введение.

В данной статье рассматриваются особенности цифрового контента при его использовании в судебном деле для установления объективного факта действительности. Анализируя требования, установленные для обеспечения подлинности доказательств, включающих цифровой контент в других правовых системах, в статье подчеркивается необходимость дополнительных правил, которые бы поддерживали болгарский суд в его судебной функции при работе с цифровыми данными.

В конце 2023 года Высший судебный совет принял поправки к двум правилам, направленным на поддержку болгарских судов в обработке электронных доказательств. Изменения касаются Положения № 6 от 3 августа 2017 года о процессуальных действиях и официальных декларациях в электронной форме [1] и Положения № 5 от 1 июня 2017 года об организации, управлении и доступе к электронным файлам дел [2], а также о сохранении доказательств и доказательственных материалов в судебных разбирательствах, а также о внутреннем обороте и хранении другой информации, обрабатываемой судебной администрацией. Эти обновления были направлены на решение фундаментальных вопросов, связанных с качеством правовой базы в области электронного управления и электронного правосудия в судебной системе.

В статье излагаются шаги, необходимые для обеспечения законности каждого этапа сбора,

использования и сохранения данных, а также методы анализа и оценки таких данных с точки зрения их существования, времени создания, проверки, авторства и содержания. Подход основан на комбинированном применении Руководства по интеграции криминалистических методов в реагирование на инциденты (специальная публикация NIST 800-86) [3], Руководства по идентификации, сбору, приобретению и сохранению цифровых доказательств (ISO/IEC 27037:2012), разработанного Объединенным техническим комитетом ISO/IEC JTC 1, Информационные технологии, Подкомитетом SC 27, Методы безопасности ИТ, и Руководства Европейского союза по электронным доказательствам [4]На основе этой методологии мы предлагаем выводы относительно понимания и защиты подлинности и надежности таких доказательств, основанные на правовых концепциях правдивости и подлинности, применяемых к цифровой сфере. Цель состоит в том, чтобы предоставить методологию и подход для обеспечения надлежащего сбора и использования электронных доказательств и процесса определения их подлинности.

Материалы и методы исследования

В данной статье определяются методы представления, сбора, защиты, анализа, хранения и архивирования электронных доказательств, при этом такие электронные данные классифицируются по существующим типам, где это применимо. Исследование основывается на возможностях современных технологий, включая отдельные методы цифровой криминалистики, применяемых в правовом контексте, в котором доказательства представляются и оцениваются. Целью является выявление объективно осуществимых подходов в отношении конкретных видов данных и связанных с ними технических и юридических параметров.

Предлагаемые методы и инструменты не ограничиваются сферой уголовного преследования; напротив, они применимы ко всем видам судебных разбирательств, в которых требуется использование электронных доказательств. Существенное значение данной работы заключается в ее потенциальной применимости даже в тех случаях, когда определенные действия суда или сторон, совершаемые в рамках процессуальных правоотношений в электронной среде, сами по себе подлежат квалификации как электронные доказательства в контексте судебного производства.

В статье обобщены передовые практики по сбору, защите, анализу и сохранению доказательств, с учетом правовых требований к технологическим характеристикам, необходимым для обеспечения объективного качества электронных доказательств в судебных целях.

В третьем разделе настоящего исследования формулируются различные понятия, относящиеся к данным, создаваемым и/или существующим в электронной среде, которые могут содержать заявления или цифровые следы выполненных действий, а также иные признаки, имеющие значение для их квалификации и оценки в качестве доказательств.

Продолжая анализ, рассматриваются вопросы доказательной ценности — то есть способности надлежащим образом собранных цифровых доказательств устанавливать факт объективной реальности, — а также проводится различие между информационной ценностью электронных данных и их доказательной силой как юридически значимых доказательств в процессе.

Результаты и их обсуждение.

В этом разделе представлены различные определения, относящиеся к электронным доказательствам, а также множество типов таких доказательств с учетом их технических характеристик и специфики правового регулирования.

Согласно определению, предусмотренному болгарским Законом об электронных документах и услугах электронной сертификации, электронное заявление представляет собой устное высказывание, представленное в цифровой форме с использованием общепринятого

стандарта преобразования, чтения и отображения информации. Такое заявление также может содержать невербальную информацию.

В соответствии со статьёй 3, пунктом 1 указанного закона, определение электронного документа [5] соответствует статье 3, пункту 35 Регламента (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года об электронной идентификации и услугах доверия для электронных транзакций на внутреннем рынке и отмене Директивы 1999/93/ЕС (OJ L 257/73, 28 августа 2014 г.) [6]. Согласно этому определению, электронный документ — это любое содержание, хранящееся в электронной форме, в частности текст, звук, изображение или аудиовизуальная запись.

Болгарское законодательство не связывает в обязательном порядке электронное заявление с его подписанием. В этом контексте возможно существование электронного заявления в составе неподписанного электронного документа. Когда электронный документ подписан, различают два аспекта: А) тип используемой электронной подписи; Б) правовые последствия её применения.

Правовой аспект различий будет рассмотрен в следующем разделе, однако здесь важно отметить, что подпись с квалифицированной электронной подписью (QES) всегда признаётся юридически эквивалентной собственноручной подписи. В то же время простая или расширенная электронная подпись (без квалификации) приобретает юридическую силу только при наличии согласия сторон, что на практике встречается значительно реже.

Данные различия имеют принципиальное значение при оценке достоверности и допустимости электронных доказательств в судебных разбирательствах, так как от них зависит, может ли представленный цифровой документ быть признан доказательством, подтверждающим конкретный юридически значимый факт. Наш закон помещает электронные заявления в среду общения, упоминая автора, держателя и получателя заявления. Однако, как мы отметили ранее, следует признать, что существует множество других типов данных, которые содержат заявления или связаны с ними, или имеют удостоверяющий характер, или любой информационный контент, который может быть значимым в качестве доказательства в различных судебных процессах и создаются или существуют в электронной среде. Существует также множество типов данных, которые представляют собой цифровые доказательства, даже не обязательно содержащие заявления.

Существует множество данных с информационной значимостью, которые могут быть собраны и использованы в судебных разбирательствах. Эти данные систематически представлены в соответствии со стандартами и описаниями, изложенными в Руководстве по интеграции криминалистических методов в специальную публикацию реагирования на инциденты 800-86 [3]. Предпринята попытка предоставить полезную информацию для совместной работы практикующих юристов и технических экспертов, что позволяет собирать и обеспечивать соответствующие доказательства, формулировать точные вопросы и запросы и проверять подлинность собранных данных.

Данные, созданные и/или существующие в электронной среде, которые могут содержать заявления или цифровые следы выполненных действий, попадают в сферу действия концепции электронного документа в соответствии с Регламентом (ЕС) № 910/2014, который определяется как «любой контент, хранящийся в электронной форме, в частности, текст или звук, визуальная или аудиовизуальная запись». Стандарт ISO/IEC 27037:2012 [7] еще больше расширяет это определение, определяя цифровые доказательства как информацию или данные, хранящиеся или передаваемые в двоичной форме, на которые можно полагаться как на доказательства. Электронные доказательства также включают цифровые данные, используемые для расследования и судебного преследования преступлений. Болгарский Уголовно-процессуальный кодекс не принимает концепцию «электронных доказательств» в ее истинном смысле. Вместо этого используется термин «компьютерные информационные данные», упомянутый в статьях

125, 135, 159, 159а и 160 Уголовно-процессуального кодекса. Согласно ст. 93, т. 22. «Компьютерные данные» означают любое представление фактов, информации или концепций в форме, которая позволяет их обработку в информационных системах, включая программу, которая способна заставить данную информационную систему выполнять определенную функцию [8]. Кроме того, термин «доказательства в электронной форме» был введен Конвенцией о киберпреступности Совета Европы (которая вступила в силу для Республики Болгария 1 августа 2005 г.) [9].

Эти данные, несомненно, могут служить доказательствами в судебных процессах. Болгарское процессуальное право еще не дало четкого определения этому особому типу доказательств, представляющему собой уникальное сочетание потенциальных аспектов вещественных доказательств, письменных заявлений и/или удостоверяющих действий. В зависимости от того, как включена запись, ее можно рассматривать либо как вещественное доказательство, либо как носитель «данных компьютерной информации» [11]. Электронные доказательства содержат данные, которые обогащают содержание сообщения. В этом смысле наши национальные правила должны учитывать дополнительные собранные данные, такие как местоположение, личность и время. Целостность данных вызывает дополнительные правовые проблемы, поскольку электронные доказательства могут включать в себя набор данных, созданных в разное время, разными способами и в разных местах. Что касается метода сбора, существуют различные технологические требования и условия, которые необходимо учитывать. Применимы общие принципы и стратегии, используемые в области кибербезопасности [12], [13], [14], [15].

Описанные здесь процедуры формируют стандартные процессы, которые должны соблюдаться в качестве принципа при обработке электронных данных, обеспечивая соблюдение остальных требований, связанных с технической реализацией принципов. Для целей судебного разбирательства, бесспорно, необходимо использовать подлинные и надежные доказательства, которые можно обоснованно утверждать, что они точно отражают объективную истину. Хотя существует подробная нормативная база и обширная судебная практика относительно надежности физических доказательств, использование электронных доказательств представляет определенные проблемы. Мы представляем методологию и использование существующих стандартов для обработки цифровых/электронных доказательств в юридических целях. Это исследование имеет особую значимость с точки зрения обеспечения и надлежащего обращения с доказательствами, поскольку оно предлагает конкретные инструменты и методические подходы, обеспечивающие своевременное реагирование при работе с цифровыми данными. Предложенная модель важна как на этапе сбора, так и на этапе хранения данных, гарантируя точность и достоверность информации, представляемой в суде.

Прежде всего, как указано в Руководстве по электронным доказательствам: Основные рекомендации для сотрудников полиции, прокуроров и судей [16], при сборе и использовании электронных данных в судебных разбирательствах, включая как уголовные, так и гражданские и административные дела, необходимо соблюдать следующие ключевые принципы:

Принцип 1: Целостность данных. Все данные должны быть защищены от изменений, повреждений или удаления на всех этапах обработки.

Принцип 2: Контрольный журнал (Audit Trail). Необходимо обеспечить возможность отслеживания всех действий, совершаемых с цифровыми доказательствами, особенно на стадии их изъятия и сбора, что предполагает документирование всех шагов.

Принцип 3: Специализированная экспертная поддержка. Работу с цифровыми доказательствами следует осуществлять с участием экспертов, обладающих соответствующими знаниями в области информационных технологий, а также компетентностью в правовой сфере. В болгарской судебной практике широко применяются судебно-компьютерные экспертизы, при

которых выводы формируются посредством двух основных процессуальных методов — обзора вещественных доказательств и экспертизы цифровых носителей [17].

Кроме того, в процессе работы с электронными доказательствами должны быть соблюдены дополнительные требования, установленные Руководящими принципами по идентификации, сбору, получению и сохранению цифровых доказательств ISO/IEC 27037:2012 [4]:

Требование 1: Валидация. Подтверждение того, что доказательства действительно отвечают заявленным целям и пригодны для использования в соответствующем процессуальном контексте. Это достигается за счёт представления объективных подтверждающих данных.

Требование 2: Верификация. Неоспоримая и функционально необходимая составляющая судебного разбирательства заключается в определении доказательной ценности представленных материалов — то есть их способности устанавливать факт, имеющий значение для разрешения спора или расследуемого дела. В этой связи использованные в настоящем исследовании определения и сформулированные принципы направлены на обеспечение такой доказательной силы применительно к электронным доказательствам.

Дальнейшее внимание в статье уделяется именно определению доказательной ценности цифровых доказательств с учетом их технологических особенностей в рамках действующего законодательства.

Для установления доказательной силы и юридической действительности электронного доказательства необходимо убедиться в следующем: наличии и существовании данных (existence); их подлинности (authenticity); целостности (integrity) пригодности и удобстве использования в процессе (usability). Формулировка этих элементов отражает влияние технологического развития на правовые подходы, связанные с установлением истины. В данном случае технические характеристики (например, неизменность и проверяемость данных) должны быть трансформированы в процессуальные категории, понятные и применимые в судебной процедуре.

Следует отметить, что вещественные доказательства, существующие в физической форме, как правило, не требуют отдельного доказательства своей целостности или пригодности для использования. Напротив, электронные доказательства предполагают необходимость внедрения специализированных процедур подтверждения технической достоверности.

Как это показано в соответствующих международных стандартах, в частности в ETSI TS 101 331 V1.8.1 [18], возможно нормативное закрепление принципа юридической действительности электронных данных как совокупности следующих элементов: подлинность (authenticity); целостность (integrity); удобство использования (usability).

Кроме того, большинство зарубежных юрисдикций при анализе цифровых доказательств исходят из трех фундаментальных принципов принятые Международной организацией по стандартизации (ИСО) в международном стандарте ISO/TR 15801:2009 [19] и стандартом ISO/IEC 27001:2013[20]:

Релевантность — данные должны быть прямо связаны с обстоятельствами дела и способствовать установлению истины. Это соответствует понятию относимости, закреплённому в болгарском процессуальном праве.

Надёжность — цифровые данные должны быть достоверными, а методы их получения и обработки — прозрачными и проверяемыми. Это требует подтверждения, что доказательство является тем, чем оно представляется.

Достаточность — объем и характер собранных цифровых доказательств должен позволять суду или органу расследования объективно оценить факты и принять обоснованное решение.

Поверх вышеописанных понятий и правовых категорий накладываются технологические принципы, имеющие особое значение при проведении экспертизы электронных доказательств. Эти принципы особенно актуальны для судебных экспертов, назначаемых судом, и подробно

описаны в международных стандартах ISO/IEC 27037:2012 [4] и ISO/IEC 27043:2015 [7], а также в руководствах для правоохранительных органов, таких как Electronic Crime Scene Investigation: A Guide for First Responders и Forensic Examination of Digital Evidence: A Guide for Law Enforcement (U.S. Department of Justice, [8]).

Основная роль экспертов заключается в том, чтобы обеспечить проверку целостности, достоверности и пригодности электронных доказательств, а также гарантировать, что все технические аспекты и процедуры были корректно трансформированы в процессуальные категории, допустимые и применимые в рамках судебного производства.В своей работе эксперты должны применять следующие ключевые технологические принципы:

Проверяемость (Auditability): Любые действия, предпринятые экспертами, должны быть документированы таким образом, чтобы независимый оценщик или иные уполномоченные стороны могли в дальнейшем провести повторную оценку и проверку их корректности. Повторяемость (Repeatability): Повторяемость подтверждается в случае, если одинаковые результаты тестирования получены одним и тем же экспертом при соблюдении следующих условий: – используется одна и та же процедура и метод измерения; – применяются одинаковые инструменты в идентичных условиях; – тест может быть вновь выполнен в любое время после первоначального теста, с получением тех же результатов. Воспроизводимость (Reproducibility): Воспроизводимость достигается, когда разные эксперты получают идентичные результаты тестирования при соблюдении следующих условий: – используется один и тот же метод измерения; – применяются разные инструменты и различные условия проведения теста; – тест можно воспроизвести независимо от первоначального времени и условий. Обоснование (Justification): Все действия, методы и решения, использованные в процессе обработки потенциальных цифровых доказательств, должны быть аргументированы и обоснованы с технической и правовой точек зрения.

Это обеспечивает как достоверность, так и допустимость таких доказательств в суде. На основе вышеупомянутых пунктов можно вывести модель для оценки того, как используются данные, существующие в электронных средах, такие как электронные доказательства, в зависимости от технологических особенностей. В качестве примера для разработки этой модели мы будем ссылаться на изменчивые данные, также известные как эфемерные данные. Изменчивые данные относятся к информации в активной системе, которая теряется при выключении компьютера, с течением времени или в результате других действий, выполняемых в системе. Во время работы операционной системы содержимое ОЗУ постоянно меняется. В любой момент ОЗУ может содержать различные типы данных и информации, которые могут представлять интерес. Несомненно, эти данные имеют информационную ценность и в этом смысле могут быть использованы в судебных разбирательствах в качестве доказательств конкретных фактов.

Сбор и сохранение этих данных технологически обусловлены таким образом, что обеспечить их доказательственную целостность либо невозможно, либо крайне сложно, учитывая необходимость соблюдения принципов Аудиторской возможности, Повторяемости и Воспроизводимости при работе с доказательствами. Представленная здесь модель демонстрирует, что существуют технологические предпосылки для электронных доказательств, которые требуют повышения правовых стандартов, связанных с их использованием в суде и оценкой их доказательной силы. Соответственно, хотя и возможно использовать информационную ценность таких данных, установление их подлинности в суде может быть невозможным из-за их технической специфики.

Заключение

В Болгарии процессуальные правила, регулирующие технологические аспекты работы с электронными доказательствами, на сегодняшний день всё ещё не установлены. С учётом

стремительного развития цифровых технологий и изменений, происходящих в общественных отношениях, назрела необходимость в чётком процессуальном ответе на вопрос: каким образом электронные доказательства должны собираться, анализироваться и оцениваться в суде.

На практике болгарские суды уже работают с электронными доказательствами, однако унифицированных руководящих принципов для их оценки не существует. Между тем, появляются новые технологические решения — в том числе основанные на блокчейне, — но процессуальные нормы, отражающие даже особенности их сбора, отсутствуют. Эти конкретные технические особенности необходимо учитывать при анализе цифровых данных и их оценке в качестве допустимых и надёжных доказательств в судебном процессе.

Описанные в статье процедуры формируют базовые стандартизированные процессы, которые должны соблюдаться как принципиальные при работе с электронными данными. Их соблюдение обеспечивает выполнение всех требований, связанных с технической реализацией принципов цифровой обработки данных: достоверности, точности, низкой стоимости, минимального вмешательства, высокой скорости и безопасности на всех этапах — от сбора до защиты.

Знание технологических предпосылок, обеспечивающих подлинность и надёжность электронных доказательств, может быть эффективно применено на всех стадиях судебного разбирательства — от инициирования сбора доказательств до их оценки и возможного оспаривания в суде. В контексте рассмотренных особенностей, связанных с удостоверением безопасности цифровых доказательств и существующей международной стандартизации, возможно практическое применение как предложенных в статье определений, так и описанных процедур, правил и принципов — в рамках болгарского судопроизводства.

В этой связи необходимо идентифицировать и унифицировать терминологию, используемую при работе с электронными доказательствами, развивать теоретические основания и методические рекомендации по практическому применению технологий в судебной деятельности, а также внедрить процессуальное регулирование, учитывающее специфику цифровых данных и принципы их допустимости, достоверности и доказательной силы.

Существующая правовая база не в полной мере отражает технологические реалии, и потому требует пересмотра и адаптации в условиях стремительно цифровизирующегося общества.

Список литературы

1. Регламент № 6 от 3 августа 2017 г. О процессуальных действиях и официальных декларациях в электронной форме. Ст. 2–8.

2. Регламент № 5 от 1 июня 2017 г. Об организации, управлении и доступе к электронным файлам дел. Ст. 5–12, 15.

3. National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). С. EC3-5–EC 3-7, EC 4-1–EC 8-1.

4. ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition, and preservation of digital evidence.

5. Закон об электронных документах и услугах электронной сертификации. Гос. газета, вып. 34, 6 апреля 2001 г. URL: https://web.apis.bg/ (дата обращения: 14.04.2025]).

6. Регламент (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 г. OJ L 257, 28.08.2014. URL: https://app.eurocases.eu/ (дата обращения: [14.04.2025]).

7. ISO/IEC 27043:2015. Incident investigation principles and processes.

8. Юруков В. Принципы, относящиеся к электронным доказательствам в уголовном судопроизводстве // De Jure. 2023. Вып. 1. URL: https://www.ceeol.com/search/article-detail?id=1112846 (дата обращения: [14.04.2025]).

9. Конвенция о киберпреступности. Будапешт, 23.XI.2001. URL:

https://rm.coe.int/1680081561 (дата обращения:14.04.2025).

10. U.S. Department of Justice. Electronic Crime Scene Investigation: A Guide for First Responders / National Institute of Justice. С. 35–46. URL: https://www.ojp.gov/pdffiles1/nij/219941.pdf (дата обращения: [14.04.2025]).

11. Иванова Г. Правовая природа частных видеозаписей как доказательств в уголовном судопроизводстве // De Jure. 2021. № 1. С. 124–132. URL: https://www.ceeol.com/search/article-detail?id=957241 (дата обращения: [14.04.2025]).

12. Shinde N., Kulkarni P. Incident response and planning: a resilient approach // Computer Fraud & Security. 2021. № 1.

13. Tatchaporn C., Thammboosadee S. A Data Masking Approach for Interpretability and Privacy in Accordance with the GDPR // Proceedings of the 11th International Conference on Advances in Information Technology. 2020.

14. Saxena N. et al. Impact and Key Issues of Insider Threats on Organizations and Critical Infrastructure // Electronics. 2020. Vol. 9. No. 9.

15. Ponta S.E., Plate H., Sabetta, A. Detection, assessment and mitigation of vulnerabilities in open-source dependencies // Empirical Software Engineering. 2020. Vol. 25. No. 5.

16. Electronic Evidence Guide: A Basic Guide for Police, Prosecutors and Judges. EU/CoE project cyber crime@ipa. URL: https://www.coe.int/en/web/cybercrime/cybercrime-ipa (дата обращения: [14.04.2025]).

17. Троянов Т. Данные, извлеченные с электронных устройств, и их ценность при расследовании преступлений // Бюллетень факультета полиции. 2021. URL: https://www.ceeol.com/search/article-detail?id=1024681 (дата обращения: [14.04.2025]).

18. ETSI. TS 101 331 V1.8.1; TS 103 307 V1.2. European Telecommunications Standards Institute. URL: https://www.etsi.org (дата обращения: [14.04.2025]).

19. ISO/TR 15801:2009. Document management – Information stored electronically – Recommendations for trustworthiness and reliability.

20. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.

References

1. Reglament № 6 ot 3 avgusta 2017 g. O processual'nyh dejstviyah i oficial'nyh deklaraciyah v elektronnoj forme. St. 2–8.

2. Reglament № 5 ot 1 iyunya 2017 g. Ob organizacii, upravlenii i dostupe k elektronnym fajlam del. St. 5–12, 15.

3. National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). C. EC3-5–EC 3-7, EC 4-1–EC 8-1.

4. ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition, and preservation of digital evidence.

5. Zakon ob elektronnyh dokumentah i uslugah elektronnoj sertifikacii. Gos. gazeta, vyp. 34, 6 aprelya 2001 g. URL: https://web.apis.bg/ (data obrashcheniya: 14.04.2025]).

6. Reglament (ES) № 910/2014 Evropejskogo parlamenta i Soveta ot 23 iyulya 2014 g. OJ L 257, 28.08.2014. URL: https://app.eurocases.eu/ (data obrashcheniya: [14.04.2025]).

7. ISO/IEC 27043:2015. Incident investigation principles and processes.

8. YUrukov V. Principy, otnosyashchiesya k elektronnym dokazatel'stvam v ugolovnom sudoproizvodstve // De Jure. 2023. Vyp. 1. URL: https://www.ceeol.com/search/article-detail?id=1112846 (data obrashcheniya: [14.04.2025]).

9. Konvenciya o kiberprestupnosti. Budapesht, 23.XI.2001. URL: https://rm.coe.int/1680081561 (data obrashcheniya:14.04.2025).

10. U.S. Department of Justice. Electronic Crime Scene Investigation: A Guide for First Responders / National Institute of Justice. C. 35–46. URL: https://www.ojp.gov/pdffiles1/nij/219941.pdf (data obrashcheniya: [14.04.2025]).

11. Ivanova G. Pravovaya priroda chastnyh videozapisej kak dokazatel'stv v ugolovnom sudoproizvodstve // De Jure. 2021. № 1. S. 124–132. URL: https://www.ceeol.com/search/article-detail?id=957241 (data obrashcheniya: [14.04.2025]).

12. Shinde N., Kulkarni P. Incident response and planning: a resilient approach // Computer Fraud & Security. 2021. № 1.

13. Tatchaporn C., Thammboosadee S. A Data Masking Approach for Interpretability and Privacy in Accordance with the GDPR // Proceedings of the 11th International Conference on Advances in Information Technology. 2020.

14. Saxena N. et al. Impact and Key Issues of Insider Threats on Organizations and Critical Infrastructure // Electronics. 2020. Vol. 9. No. 9.

15. Ponta S.E., Plate H., Sabetta, A. Detection, assessment and mitigation of vulnerabilities in open-source dependencies // Empirical Software Engineering. 2020. Vol. 25. No. 5.

16. Electronic Evidence Guide: A Basic Guide for Police, Prosecutors and Judges. EU/CoE project cyber crime@ipa. URL: https://www.coe.int/en/web/cybercrime/cybercrime-ipa (data obrashcheniya: [14.04.2025]).

17. Troyanov T. Dannye, izvlechennye s elektronnyh ustrojstv, i ih cennost' pri rassledovanii prestuplenij // Byulleten' fakul'teta policii. 2021. URL: https://www.ceeol.com/search/article-detail?id=1024681 (data obrashcheniya: [14.04.2025]).

18. ETSI. TS 101 331 V1.8.1; TS 103 307 V1.2. European Telecommunications Standards Institute. URL: https://www.etsi.org (data obrashcheniya: [14.04.2025]).

19. ISO/TR 15801:2009. Document management – Information stored electronically – Recommendations for trustworthiness and reliability.

20. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.

ЭЛЕКТРОНДЫҚ ОРТАДАҒЫ ЦИФРЛЫҚ ДЕРЕКТЕР МЕН ІЗДЕР-БОЛГАР СОТЫНДА ДӘЛЕЛ РЕТІНДЕ ПАЙДАЛАНУ МҮМКІНДІГІ

БАНКОВА Д.*, ДИМИТРОВ В.

***Банкова Добромира** – Докторант, «Әулие Клемент Охрид» София университеті, София қ., Болгария
E-mail: bankovagan@fmi.uni-sofia.bg, https://orcid.org/0000-0002-9261-2842
Димитров Владимир – Профессор, «Әулие Клемент Охрид» София университеті, София қ., Болгария
E-mail: cht@fmi.uni-sofia.bg, https://orcid.org/0000-0002-7441-253X

Аңдатпа. Қазіргі қоғамды цифрландыру құқықтық қатынастарға қатысушылар арасындағы өзара іс-қимыл тәсілін, оның ішінде заңды маңызы бар ақпаратты қалыптастыру, беру және сақтау тәсілдерін айтарлықтай өзгертті. Цифрлық технологиялар мен электрондық коммуникациялардың өсіп келе жатқан рөлі дәлелдемелерді жинауға, тексеруге және бағалауға, әсіресе сот ісін жүргізуде дәстүрлі құқықтық тәсілдерді қайта қарауды қажет етеді.

Болгарияда соңғы жылдары құқықтық жүйені цифрлық орта жағдайларына бейімдеуге бағытталған іс жүргізу заңнамасында елеулі өзгерістер қабылданды. Жалпы нормативтік-құқықтық базаның болуына қарамастан, құқық қолдану практикасында айтарлықтай олқылықтар сақталады, әсіресе цифрлық іздерді, метадеректерді, уақытша сезімталдық деректерін (мысалы, жедел жады) және басқа да стандартты емес электронды тасымалдаушыларды бағалауға қатысты. Мәселе тек осындай деректерді алудың және сақтаудың техникалық қабілетінде ғана емес, сонымен бірге объективті шындықты орнату контекстінде олардың дәлелді күшін заңды түрде түсіндіруде жатыр. Бұл зерттеудің мақсаты-Болгар сот ісін жүргізуде цифрлық деректерді дәлел ретінде қолдану мүмкіндіктерін талдау, қолданыстағы нормативтік және практикалық кедергілерді анықтау, сондай-ақ электрондық дәлелдемелердің заңды рұқсат етілуін, дұрыстығын және қайталануын қамтамасыз ететін әдістемені ұсыну. Осы жұмыс шеңберінде

халықаралық техникалық стандарттар мен сот сараптамасының қағидаттарын ұлттық құқықтық практикамен интеграциялауға әрекет жасалуда, бұл Болгар сот төрелігінде цифрлық дәлелдемелермен жұмысты одан әрі біріздендіру және стандарттау үшін негіз құруға мүмкіндік береді.

Түйін сөздер: сандық деректер, электрондық дәлелдемелер, сот талқылауы, метадеректер, деректердің тұтастығы, білікті электрондық қолтаңба.

DIGITAL DATA AND TRACES IN AN ELECTRONIC ENVIRONMENT - POSSIBILITIES OF USING AS EVIDENCE IN A BULGARIAN COURT

BANKOVA D.*, DIMITROV V.

***Bankova Dobromira** – Doctoral student, St. Kliment Ohridski Sofia University, Sofia, Bulgaria
E-mail: bankovagan@fmi.uni-sofia.bg, https://orcid.org/0000-0002-9261-2842
Dimitrov Vladimir – Professor, St. Kliment Ohridski Sofia University, Sofia, Bulgaria
E-mail: cht@fmi.uni-sofia.bg, https://orcid.org/0000-0002-7441-253X

Abstract. The digitalization of modern society has significantly changed the way in which participants in legal relations interact, including the ways in which legally relevant information is formed, transmitted, and stored. The increasing role of digital technologies and electronic communications necessitates a rethink of traditional legal approaches to the collection, verification and evaluation of evidence, especially in court proceedings.

In recent years, Bulgaria has adopted significant changes in procedural legislation aimed at adapting the legal system to the digital environment. Nevertheless, despite the existence of a common regulatory framework, significant gaps remain in law enforcement practice, especially with regard to the assessment of digital footprints, metadata, time-sensitive data (for example, RAM) and other non-standard electronic media. The problem lies not only in the technical ability to extract and store such data, but also in the legal interpretation of their evidentiary value in the context of establishing objective truth. The purpose of this study is to analyze the possibilities of using digital data as evidence in Bulgarian legal proceedings, identify existing regulatory and practical barriers, and propose a methodology to ensure the legal admissibility, reliability, and reproducibility of electronic evidence. Within the framework of this work, an attempt is being made to integrate international technical standards and principles of forensic examination with national legal practice, which will create the basis for further unification and standardization of work with digital evidence in Bulgarian justice.

Key words: digital data, electronic evidence, judicial proceedings, metadata, data integrity, qualified electronic signature.