



ОСНОВЫ ТЕОРИИ И НОРМАТИВНАЯ БАЗА ОЦЕНКИ ЭЛЕКТРОННЫХ
ДОКАЗАТЕЛЬСТВ

GUO FEI

AllBright Law Offices

E-mail: guoffei@yandex.ru

Аннотация. В тезисе рассматриваются теоретические основы и нормативно-правовые аспекты оценки электронных доказательств в современном судопроизводстве. Раскрываются понятие электронных доказательств, их основные признаки, критерии допустимости, относимости, достоверности и достаточности. Особое внимание уделяется вопросам установления подлинности цифровой информации, обеспечения её целостности, соблюдения порядка получения и хранения, а также использования специальных знаний при исследовании электронных данных. Обосновывается необходимость совершенствования правового регулирования электронных доказательств в условиях цифровизации общественных отношений.

Ключевые слова: электронные доказательства, цифровая информация, судопроизводство, нормативно-правовое регулирование, допустимость доказательств, достоверность, цифровая криминалистика, электронные документы.

Введение. Развитие информационно-коммуникационных технологий и цифровизация общественных отношений оказывают существенное влияние на деятельность правоохранительных органов и судебных учреждений. Электронная переписка, сообщения в мессенджерах, аудио- и видеозаписи, сведения из информационных систем, данные электронных платежей и другие цифровые материалы всё чаще приобретают значение при установлении фактических обстоятельств дела. В связи с этим особую актуальность приобретает исследование теоретических основ и нормативной базы оценки электронных доказательств.

Электронные доказательства отличаются от традиционных источников доказательственной информации способом создания, хранения, передачи и воспроизведения. Их содержание может быть изменено, удалено или скопировано без очевидных внешних признаков вмешательства. Кроме того, при оценке цифровых данных необходимо учитывать технические характеристики устройств, метаданные, временные отметки, способы идентификации пользователя и обстоятельства получения информации. Поэтому использование электронных доказательств требует не только юридической оценки, но и применения специальных технических знаний. Цель настоящего исследования заключается в раскрытии теоретических положений оценки электронных доказательств и определении основных направлений нормативно-правового регулирования их получения, проверки и использования в судопроизводстве.



Основная часть

Теоретические основы оценки электронных доказательств. Электронные доказательства представляют собой сведения, зафиксированные в цифровой форме и используемые в установленном законом порядке для установления обстоятельств, имеющих значение для разрешения юридического спора или расследования правонарушения. В зависимости от законодательства конкретного государства такие сведения могут рассматриваться как самостоятельная категория доказательств либо исследоваться в рамках предусмотренных процессуальным законом видов доказательственной информации.

Теоретической основой оценки электронных доказательств выступают общие принципы доказывания. К ним относятся относимость, допустимость, достоверность и достаточность доказательств. Каждый из этих критериев имеет самостоятельное значение. Относимость означает наличие связи электронных данных с обстоятельствами, которые подлежат установлению по делу. Например, электронная переписка может иметь значение для подтверждения факта заключения соглашения, направления уведомления или согласования определённых условий. Допустимость предполагает соблюдение предусмотренных законом требований к получению, закреплению и представлению доказательственной информации. Даже содержательно значимые цифровые данные могут вызвать процессуальные вопросы, если они получены с нарушением установленных требований. Достоверность характеризует соответствие электронных данных действительным обстоятельствам. При её установлении исследуются происхождение информации, целостность файла, наличие признаков изменения, соответствие метаданных и другие обстоятельства. Достаточность предполагает возможность совокупности доказательств обосновать соответствующие фактические выводы. Как правило, электронные данные целесообразно сопоставлять с другими материалами дела, поскольку отдельный цифровой объект не всегда позволяет однозначно установить все обстоятельства. Таким образом, оценка электронных доказательств должна осуществляться комплексно, с учётом как процессуальных требований, так и технических особенностей цифровой информации.

В Республике Узбекистан правовая оценка электронных доказательств должна осуществляться с учётом соответствующего вида судопроизводства и применимых процессуальных норм. Важное значение имеют Гражданский процессуальный кодекс Республики Узбекистан, Экономический процессуальный кодекс Республики Узбекистан и Уголовно-процессуальный кодекс Республики Узбекистан. Конкретные положения каждого кодекса необходимо применять с учётом категории дела, способа получения цифровых данных и предусмотренной законом формы их представления. Дополнительное значение имеют Закон Республики Узбекистан «Об электронном документообороте» и Закон Республики Узбекистан «Об электронной цифровой подписи». Эти нормативные акты формируют правовые условия использования



электронных документов и электронной цифровой подписи, в том числе при установлении происхождения документа и проверке его юридической значимости. При этом наличие электронной подписи само по себе не подтверждает автоматически истинность всех сведений, содержащихся в документе: содержание и относимые обстоятельства должны оцениваться в совокупности с другими материалами. На международном уровне важное значение имеет Типовой закон ЮНСИТРАЛ об электронной торговле 1996 года, закрепляющий подход, согласно которому юридическая сила информации не должна отрицаться исключительно по причине её представления в электронной форме. Данный документ имеет модельный характер и применяется в национальном правовом порядке в той мере, в какой его положения реализованы соответствующим законодательством. Следовательно, нормативная база оценки электронных доказательств должна обеспечивать баланс между эффективным использованием цифровых технологий, соблюдением процессуальных гарантий участников дела и защитой прав человека.

Основные проблемы оценки электронных доказательств. Одной из ключевых проблем является установление подлинности цифровой информации. Электронный файл может быть скопирован, отредактирован или представлен без исходных технических данных. В связи с этим важно установить источник информации, способ её получения и наличие признаков изменения после создания. Второй проблемой выступает обеспечение целостности цифровых данных. При работе с электронными носителями применяются технические процедуры фиксации состояния информации, создания криминалистических копий и вычисления контрольных хеш-сумм. Хеш-сумма позволяет проверить, изменилось ли содержимое файла между двумя моментами сравнения, однако сама по себе не доказывает, что первоначальный файл был подлинным или создан конкретным лицом. Третья проблема связана с идентификацией автора электронного сообщения. Использование определённой учётной записи или устройства не всегда означает, что сообщение отправлено именно владельцем соответствующей записи. Поэтому необходимо учитывать сведения о доступе к устройству, журналы событий, данные информационной системы и иные подтверждающие обстоятельства.

Отдельного внимания требует соблюдение прав участников судопроизводства. Получение электронной переписки, данных устройств и сведений из облачных сервисов должно осуществляться с соблюдением установленных законом процедур, требований о защите персональных данных и, когда это необходимо, правил получения разрешения уполномоченного органа или суда.

Для повышения качества оценки электронных доказательств целесообразно развивать следующие направления: Совершенствовать процессуальные нормы, регулирующие получение, фиксацию, представление и исследование цифровой информации. Разрабатывать единые методические рекомендации по сохранению целостности электронных данных. Расширять применение специальных знаний и



судебных компьютерно-технических экспертиз. Повышать цифровую грамотность судей, следователей, адвокатов и других участников процесса. Обеспечивать документирование всех существенных операций с цифровыми носителями и файлами. Развивать международное сотрудничество при получении электронных данных, находящихся на серверах за пределами национальной юрисдикции.

Закключение. Таким образом, оценка электронных доказательств представляет собой комплексный процесс, включающий юридическую проверку и техническое исследование цифровой информации. Её эффективность зависит от соблюдения критериев относимости, допустимости, достоверности и достаточности, а также от надлежащего установления происхождения и целостности электронных данных. Нормативно-правовая база должна определять порядок получения, фиксации, хранения, представления и исследования электронных доказательств, одновременно обеспечивая защиту процессуальных прав участников судопроизводства. Для Республики Узбекистан актуальными направлениями остаются согласование процессуальных норм с развитием цифровых технологий, совершенствование методик компьютерно-технической экспертизы и повышение профессиональной компетентности специалистов. Перспективы дальнейших исследований связаны с разработкой практических критериев оценки электронной переписки, данных социальных сетей, облачных хранилищ, цифровых журналов событий и материалов, созданных с использованием искусственного интеллекта. Комплексное решение этих задач будет способствовать повышению обоснованности судебных решений и укреплению доверия к электронным доказательствам.

Список использованной литературы

1. Закон Республики Узбекистан «Об электронном документообороте» от 29 апреля 2004 года № 611-II.
2. Закон Республики Узбекистан «Об электронной цифровой подписи» от 12 октября 2022 года № ЗРУ-793.
3. Типовой закон ЮНСИТРАЛ об электронной торговле. Принят Комиссией ООН по праву международной торговли в 1996 году.
4. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. — Waltham: Academic Press, 2011.
5. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.