

ДОКАЗАТЕЛЬСТВЕННАЯ СИЛА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В МЕЖДУНАРОДНОМ КОММЕРЧЕСКОМ АРБИТРАЖЕ: ГРАЖДАНСКО- ПРАВОВЫЕ ПОСЛЕДСТВИЯ КИБЕРИНЦИДЕНТОВ

Кайбылдаева Бегаим Мухитовна

Независимый исследователь,

Ташкентский государственный юридический университет

Эл. почта: begaimkaibylldaeva@gmail.com

<https://doi.org/10.5281/zenodo.21065042>

Введение. Стремительная цифровизация международной коммерции повлекла за собой фундаментальный сдвиг в структуре доказательственной базы арбитражных разбирательств: электронные договоры, переписка по электронной почте, метаданные транзакций и записи распределённых реестров всё чаще составляют центральный доказательственный материал в международных коммерческих спорах. Вместе с тем нарастающая угроза киберинцидентов, под которыми понимаются несанкционированный доступ к информационным системам, их компрометация или умышленное уничтожение данных, порождает серьёзные правовые вопросы относительно достоверности, целостности и допустимости электронных документов в арбитражном процессе.

Гражданско-правовые последствия киберинцидентов в контексте арбитражного доказывания остаются недостаточно изученными как в международной доктрине, так и в узбекском праве. Применительно к Республике Узбекистан данная проблематика приобретает особую актуальность в условиях активной цифровой трансформации экономики и последовательного совершенствования законодательства об электронных документах и кибербезопасности.

Настоящая работа исследует доказательственный статус электронных документов в международном коммерческом арбитраже, гражданско-правовые механизмы распределения ответственности при киберинцидентах, затрагивающих доказательственную базу, а также специфику национального регулирования в данной области.

Электронные документы как доказательства в международном арбитраже: правовой режим. В отличие от государственных судов, жёстко связанных национальными процессуальными нормами доказывания, международный коммерческий арбитраж исходит из широкой дискреции трибунала при оценке доказательств. Согласно статье 34 Закона Республики Узбекистан от 16 февраля 2021 г. № ЗРУ-674 «О международном коммерческом арбитраже», арбитражный суд вправе самостоятельно определять допустимость, относимость и существенность любого доказательства, включая электронные документы.¹

На международном уровне стандарты работы с электронными доказательствами систематизированы в Правилах МБА о получении доказательств в международном арбитраже 2020 года (IBA Rules on the Taking of Evidence in International Arbitration),

¹ Закон РУз «О международном коммерческом арбитраже» от 16.02.2021 г. № ЗРУ-674, ст. 34. <https://lex.uz/docs/5294087>

которые допускают представление доказательств в электронной форме и содержат специальные нормы об их раскрытии и сохранении.²

Правовую основу легитимности электронных документов в Узбекистане образует Закон от 29 апреля 2004 г. № 611-II «Об электронном документообороте». Согласно статье 5 Закона, электронным документом признаётся информация, зафиксированная в электронной форме и подтверждённая электронной цифровой подписью; в соответствии со статьёй 7 такой документ приравнивается к документу на бумажном носителе и обладает одинаковой с ним юридической силой.³

Существенным дополнением служит Закон от 12 октября 2022 г. № ЗРУ-793 «Об электронной цифровой подписи» (принят Законодательной палатой 26 июля 2022 г., одобрен Сенатом 13 сентября 2022 г.), статья 4 которого устанавливает условия равнозначности ЭЦП собственноручной подписи, а статья 5 определяет требования к средствам ЭЦП.⁴

Гражданский процессуальный кодекс Республики Узбекистан, утверждённый Законом от 22 января 2018 г. № ЗРУ-460, дополненный Законом от 21 ноября 2024 г. № ЗРУ-1003, закрепил в статьях 89¹-89⁴ понятия электронных данных и цифровых доказательств, установив процедуры их представления, обязанности по раскрытию и условия осмотра судом.⁵

Киберинциденты и их влияние на доказательственную базу: правовая квалификация. Закон Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 «О кибербезопасности» (вступил в силу 17 июля 2022 г.; принят Законодательной палатой 25 февраля 2022 г., одобрен Сенатом 17 марта 2022 г.) содержит в статье 3 определение инцидента кибербезопасности как события в киберпространстве, приведшего к сбоям в работе информационных систем и нарушениям доступности, целостности информации или возможности её свободного использования. Статья 14 Закона обязывает государственные органы и организации принимать меры по предотвращению хищения и фальсификации данных и уведомлять уполномоченный государственный орган о кибератаках.⁶

С точки зрения арбитражного доказывания киберинциденты порождают три взаимосвязанные правовые проблемы. Первая касается допустимости скомпрометированных документов: если несанкционированное воздействие могло изменить содержимое электронных файлов, подлинность таких документов становится предметом спора. Вторая связана с бременем доказывания факта компрометации и причинно-следственной связи между инцидентом и предполагаемым изменением документа. Третья охватывает гражданско-правовую ответственность стороны, не обеспечившей надлежащую защиту своих информационных систем, за последствия утраты или искажения доказательно значимых данных.

2 IBA Rules on the Taking of Evidence in International Arbitration 2020. International Bar Association. <https://www.ibanet.org/ibarulesevidence>

3 Закон РУз «Об электронном документообороте» от 29.04.2004 г. № 611-II, ст. 5, 7. <https://lex.uz/docs/165074>

4 Закон РУз «Об электронной цифровой подписи» от 12.10.2022 г. № ЗРУ-793, ст. 4, 5. <https://lex.uz/ru/docs/6234906>

5 ГПК РУз (в ред. Закона от 21.11.2024 г. № ЗРУ-1003), ст. 89¹-89⁴. <https://lex.uz/ru/docs/3517334>

6 Закон РУз «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764, ст. 3, 14, 15. <https://lex.uz/ru/docs/5960609>

Постановление Президента Республики Узбекистан от 31 мая 2023 г. № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры» конкретизировало требования к защите данных в ключевых отраслях экономики. Несоблюдение данных требований может быть квалифицировано как нарушение обязанности по обеспечению сохранности доказательно значимой информации при наличии разумного предвидения арбитражного разбирательства.⁷

Гражданско-правовые последствия киберинцидентов для арбитражного разбирательства. Утрата или фальсификация электронных доказательств вследствие кибератаки способна повлечь три группы гражданско-правовых последствий. Первая связана с договорной ответственностью: при наличии в контракте условий о кибербезопасности или хранении документации их нарушение влечёт ответственность стороны-нарушителя в соответствии с нормами об ответственности за ненадлежащее исполнение обязательств. Вторая группа затрагивает доказательственные презумпции: трибунал вправе делать неблагоприятные выводы из непредставления стороной доказательств, хранившихся в скомпрометированной системе, если эта сторона не приняла разумных мер к их восстановлению или резервированию. Третья группа охватывает деликтную ответственность за умышленное уничтожение доказательств третьими лицами.

В международной арбитражной практике сложилась концепция уничтожения доказательств (spoliation): трибуналы применяют санкции против стороны, не обеспечившей сохранность электронных доказательств после возникновения разумного предвидения арбитражного разбирательства. Принятый Закон от 21 ноября 2024 г. № ЗРУ-1003 (принят Законодательной палатой 27 августа 2024 г., одобрен Сенатом 24 октября 2024 г.) формирует национальную правовую основу для надлежащей фиксации и сохранения цифровых доказательств в процессуальных документах.⁸

В доктрине международного коммерческого арбитража устоялся консенсус о том, что сторона, представляющая электронный документ в качестве доказательства, несёт первичное бремя доказывания его аутентичности. При наличии убедительных данных о киберинциденте в соответствующий период трибунал может назначить техническую экспертизу либо применить стандарт баланса вероятностей к оценке документа.⁹

Практические механизмы обеспечения доказательственной силы электронных документов. Международный опыт выработал ряд технических и правовых инструментов снижения рисков, связанных с киберинцидентами в арбитражных разбирательствах. Использование квалифицированных временных меток, подтверждённых аккредитованными удостоверяющими центрами, хэширования документов и сквозного шифрования переписки существенно повышает устойчивость электронных доказательств к оспариванию. В Узбекистане правовую основу для

⁷ Born, G. B. (2021). International Commercial Arbitration (3rd ed.). Kluwer Law International.

⁸ Постановление Президента РУз от 31.05.2023 г. № ПП-167. <https://lex.uz/ru/docs/6479197>

⁹ Закон РУз от 21.11.2024 г. № ЗРУ-1003. <https://lex.uz/ru/docs/7228823>

применения таких инструментов создают Закон об электронном документообороте № 611-II, ст. 16-17, а также Закон об ЭЦП № ЗРУ-793, ст. 7.¹⁰

Для узбекских коммерческих субъектов, вовлечённых в международные сделки, практически важным является включение в договоры положений об обязательном резервном копировании документации, использовании систем управления документами с фиксацией истории изменений, а также о процедурах уведомления контрагента в случае кибератаки. Требование о резервном копировании данных с хранением копий не менее трёх последних месяцев закреплено в статье 15 Закона о кибербезопасности № ЗРУ-764.¹¹

Применительно к Ташкентскому международному арбитражному центру представляется целесообразным введение в регламент специальных процедур работы с электронными доказательствами, включая механизм безопасной депозитной сдачи их на хранение по аналогии с практикой ведущих арбитражных институтов.¹²

Заключение. Электронные документы прочно вошли в арсенал доказательственных средств международного коммерческого арбитража, однако сопряжённые с ними риски киберинцидентов ставят перед правоприменителями комплекс актуальных правовых вопросов. В системе узбекского права формируется необходимая законодательная база: Закон об электронном документообороте № 611-II (2004), Закон о кибербезопасности № ЗРУ-764 (2022), Закон об ЭЦП № ЗРУ-793 (2022) и Закон о цифровых доказательствах № ЗРУ-1003 (2024) в совокупности создают правовую инфраструктуру для защиты электронной доказательственной базы.

В этой связи представляется целесообразным: дополнить Закон о международном коммерческом арбитраже № ЗРУ-674 специальными нормами об оценке электронных доказательств; разработать методические рекомендации ТМАЦ по работе с цифровыми доказательствами; содействовать участию Республики Узбекистан в разработке международных стандартов в сфере электронных доказательств в рамках ЮНСИТРАЛ.

Перспективными направлениями дальнейших исследований представляются изучение практики работы с электронными доказательствами в ТМАЦ, сравнительный анализ регулирования в государствах Центральной Азии, а также разработка типовых договорных положений о киберзащите доказательственной базы для международных коммерческих контрактов.

Adabiyotlar, References, Литературы:

1. Born, G. B. (2021). *International Commercial Arbitration* (3rd ed.). Kluwer Law International.
2. Schreuer, C., Malintoppi, L., Reinisch, A., & Sinclair, A. (2009). *The ICSID Convention: A Commentary* (2nd ed.). Cambridge University Press.
3. UNCTAD. (2023). *World Investment Report 2023*. United Nations. <https://unctad.org/wir2023>
4. IBA Rules on the Taking of Evidence in International Arbitration. (2020). International

¹⁰ Schreuer, C. et al. (2009). *The ICSID Convention: A Commentary* (2nd ed.). Cambridge University Press.

¹¹ UNCTAD. (2023). *World Investment Report 2023*. United Nations. <https://unctad.org/wir2023>

¹² Закон «Об электронном документообороте» № 611-II, ст. 16-17; Закон «Об ЭЦП» № ЗРУ-793, ст. 7. <https://lex.uz/docs/165074>

Bar Association. <https://www.ibanet.org/ibarulesevidence>

5. Республика Узбекистан. (2004). Закон «Об электронном документообороте» от 29 апреля 2004 г. № 611-II. <https://lex.uz/docs/165074>
6. Республика Узбекистан. (2021). Закон «О международном коммерческом арбитраже» от 16 февраля 2021 г. № ЗРУ-674. <https://lex.uz/docs/5294087>
7. Республика Узбекистан. (2022). Закон «О кибербезопасности» от 15 апреля 2022 г. № ЗРУ-764 (вступил в силу 17 июля 2022 г.). <https://lex.uz/ru/docs/5960609>
8. Республика Узбекистан. (2022). Закон «Об электронной цифровой подписи» от 12 октября 2022 г. № ЗРУ-793. <https://lex.uz/ru/docs/6234906>
9. Республика Узбекистан. (2023). Постановление Президента «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов КИИ» от 31 мая 2023 г. № ПП-167. <https://lex.uz/ru/docs/6479197>
10. Республика Узбекистан. (2024). Закон «О внесении изменений, направленных на совершенствование системы работы с цифровыми доказательствами» от 21 ноября 2024 г. № ЗРУ-1003. <https://lex.uz/ru/docs/7228823>
11. Гражданский процессуальный кодекс Республики Узбекистан, утв. Законом РУз от 22 января 2018 г. № ЗРУ-460 (ст. 89¹-89⁴ введены Законом № ЗРУ-1003 от 21 ноября 2024 г.). <https://lex.uz/ru/docs/3517334>