



ГРАЖДАНСКО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ АРБИТРАЖНЫХ ИНСТИТУТОВ ЗА НАРУШЕНИЕ КИБЕРБЕЗОПАСНОСТИ: ВОПРОСЫ ДЕЛИКТНОГО И ДОГОВОРНОГО РЕГУЛИРОВАНИЯ

Кайбылдаева Бегаим Мухитовна

Независимый исследователь, Ташкентский государственный
юридический университет.

Э- почта: begaimkaibyladaeva@gmail.com

<https://doi.org/10.5281/zenodo.20622782>

ARTICLE INFO

Received: 04th June 2026

Accepted: 06th June 2026

Online: 09th June 2026

KEYWORDS

Арбитражный институт как субъект гражданско-правовых отношений занимает особое положение: с одной стороны, он действует на основании административного соглашения со сторонами спора, с другой несёт публично значимые функции по обеспечению надлежащего правосудия в сфере частного права

ABSTRACT

Цифровизация процедур международного арбитража повлекла за собой формирование принципиально нового класса правовых рисков, связанных с уязвимостью информационных систем арбитражных институтов. Хранение конфиденциальных материалов дел, персональных данных сторон и арбитров, а также коммуникационные платформы для удалённых слушаний стали объектами систематических кибератак. По данным Международной торговой палаты, только за 2022-2023 годы было зафиксировано несколько случаев компрометации данных в ведущих арбитражных центрах мира. Это обуславливает практическую необходимость чёткого разграничения оснований гражданско-правовой ответственности арбитражных институтов в деликтном и договорном измерениях.

Введение. Цифровизация процедур международного арбитража повлекла за собой формирование принципиально нового класса правовых рисков, связанных с уязвимостью информационных систем арбитражных институтов. Хранение конфиденциальных материалов дел, персональных данных сторон и арбитров, а также коммуникационные платформы для удалённых слушаний стали объектами систематических кибератак. По данным Международной торговой палаты, только за 2022-2023 годы было зафиксировано несколько случаев компрометации данных в ведущих арбитражных центрах мира. Это обуславливает практическую необходимость чёткого разграничения оснований гражданско-правовой ответственности арбитражных институтов в деликтном и договорном измерениях.

Арбитражный институт как субъект гражданско-правовых отношений занимает особое положение: с одной стороны, он действует на основании административного соглашения со сторонами спора, с другой несёт публично значимые функции по обеспечению надлежащего правосудия в сфере частного права. Двойственность этого статуса определяет сложность квалификации его ответственности за нарушения кибербезопасности. В настоящей работе рассматриваются основания и условия такой

ответственности применительно к действующим нормам гражданского и информационного права, включая законодательство Республики Узбекистан.

Правовая природа отношений между арбитражным институтом и сторонами спора. Отношения, возникающие между арбитражным институтом и сторонами арбитражного разбирательства, опосредуются, как правило, двумя взаимосвязанными договорными конструкциями: арбитражным соглашением (арбитражной оговоркой) и административным договором об оказании арбитражных услуг. Последний регулирует организационные условия проведения разбирательства, в том числе порядок хранения и защиты документации, обеспечение конфиденциальности и предоставление технологической инфраструктуры для электронного взаимодействия сторон и арбитров.

В доктрине международного коммерческого арбитража административный договор квалифицируется как смешанный договор возмездного оказания услуг, включающий элементы поручения, хранения и информационного обслуживания.¹ Применительно к праву Республики Узбекистан данная конструкция подпадает под действие главы 36 Гражданского кодекса Республики Узбекистан о возмездном оказании услуг, а также специальных норм Закона «О международном коммерческом арбитраже» 2021 года, регламентирующих правовой статус арбитражных учреждений.²

Из договорной природы данных отношений вытекают конкретные обязательства арбитражного института по обеспечению безопасности информации. К числу таковых относятся: соблюдение конфиденциальности материалов дела, защита персональных данных участников разбирательства, поддержание работоспособности и защищённости электронных систем связи, а также принятие разумных мер по предотвращению несанкционированного доступа к информационным ресурсам института. Нарушение любого из перечисленных обязательств способно повлечь как договорную, так и деликтную ответственность в зависимости от характера причинённого вреда.

Договорная ответственность арбитражного института за нарушение кибербезопасности. Договорная ответственность арбитражного института наступает при установлении следующих условий: наличия действительного административного договора; ненадлежащего исполнения вытекающих из него обязательств по защите информации; причинно-следственной связи между ненадлежащим исполнением и наступившими убытками; а также вины должника, если иное прямо не предусмотрено договором или законом.

Центральным вопросом при оценке ненадлежащего исполнения является стандарт должной осмотрительности в области информационной безопасности, которому обязан соответствовать арбитражный институт. В международной практике данный стандарт формируется на основе: требований регуляторов в области защиты данных (в частности, Общего регламента по защите данных ЕС GDPR),³ рекомендаций

¹Schreuer C., Malintoppi L., Reinisch A., Sinclair A. The ICSID Convention: A Commentary (2nd ed.). Cambridge University Press, 2009. P. 1–1082.

²Born G.B. International Commercial Arbitration (3rd ed.). Kluwer Law International, 2021. P. 1–4800.

³Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR) // OJ L 119. 4.5.2016. P. 1–88.

МТП и ЮНСИТРАЛ по применению информационных технологий в арбитраже,⁴ а также общепринятых отраслевых стандартов в сфере кибербезопасности (ISO/IEC 27001, NIST Cybersecurity Framework). В Республике Узбекистан аналогичные требования закреплены в Законе «Об информатизации» 2003 года и Законе «О персональных данных» 2019 года, а также в Законе Республики Узбекистан «О кибербезопасности» 2022 года.⁵⁶⁷

Особую проблему представляют оговорки об ограничении ответственности, традиционно включаемые в регламенты ведущих арбитражных институтов (МТП, ЛМТС, МЦУИС). Как правило, такие оговорки исключают ответственность института и арбитров за действия или бездействие в ходе разбирательства, однако их распространение на нарушения кибербезопасности вопрос дискуссионный. В ряде правовых систем ограничение ответственности за умышленные действия или грубую небрежность признаётся ничтожным; иные правовые порядки допускают такое ограничение при условии надлежащего уведомления стороны. В праве Узбекистана согласно статье 349 ГК РУз соглашение об устранении ответственности за умышленное нарушение обязательства ничтожно, что создаёт нижнюю границу допустимого освобождения от ответственности.⁸

Деликтная ответственность за нарушение кибербезопасности. Деликтная ответственность арбитражного института может наступить независимо от наличия договорных отношений, в частности в пользу третьих лиц, чьи персональные данные или коммерческие тайны стали известны вследствие кибератаки. Основания деликтной ответственности в данном контексте определяются нормами генерального деликта (ст. 985 ГК РУз) и специальными нормами об ответственности за нарушение законодательства о персональных данных.

Ключевым элементом состава деликта в сфере кибербезопасности является противоправность, которая в данном случае выражается в нарушении нормативно установленных стандартов защиты информации. Согласно концепции небрежности, выработанной в англо-американской судебной практике и воспринятой в ряде континентальных правовых порядков, ответственность наступает при доказанности: (1) наличия обязанности проявлять должную осмотрительность по отношению к истцу; (2) нарушения этой обязанности; (3) причинно-следственной связи; (4) реального ущерба.⁹

⁴Restatement (Second) of Torts § 552 (Am. Law Inst. 1977); Prosser W.L., Keeton W.P. Prosser and Keeton on the Law of Torts (5th ed.). West Publishing, 1984. P. 700–740.

⁵UNCITRAL Notes on Organizing Arbitral Proceedings (3rd ed., 2016). United Nations. URL: <https://uncitral.un.org> (дата обращения: 20.05.2025).

⁶Закон Республики Узбекистан «О международном коммерческом арбитраже» от 16 февраля 2021 г. № ЗРУ-674 // Национальная база данных законодательства Республики Узбекистан. 2021. № 03/21/674/0123.

⁷Директива 2016/1148/ЕС Европейского парламента и Совета от 6 июля 2016 г. о мерах по высокому общему уровню безопасности сетей и информационных систем (Директива NIS) // OJ L 194. 19.7.2016. P. 1–30.

⁸Гражданский кодекс Республики Узбекистан от 29 августа 1996 г. (с изм. и доп. по сост. на 2025 г.) // Ведомости Олий Мажлиса Республики Узбекистан. 1997. № 2. Ст. 36 (ст. 985–988, 1005–1010).

⁹Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 г. № ЗРУ-547 // Собрание законодательства Республики Узбекистан. 2019. № 27. Ст. 634.

Применительно к арбитражным институтам существенной специфической чертой является доктрина иммунитета арбитра (и института), которая в ряде юрисдикций прежде всего основанных на принципе common law предоставляет широкую защиту от деликтных исков, возникающих из осуществления квазисудебных функций. Вместе с тем иммунитет, как правило, не распространяется на административные функции института, в том числе на организацию технической инфраструктуры и защиту данных. Директива NIS ЕС 2016 года закрепляет позитивные обязательства по безопасности цифровой инфраструктуры для широкого круга операторов услуг, что создаёт нормативный ориентир и для арбитражных учреждений, расположенных или обрабатывающих данные на территории ЕС.¹⁰

Конкуренция деликтного и договорного требований: коллизионные вопросы и выбор применимого права. При наличии административного договора между арбитражным институтом и сторонами спора возникает типичная ситуация конкуренции договорного и деликтного требований (*concurrency d'actions*). В гражданском праве Узбекистана принцип недопустимости «деликтизации» договорных отношений закреплён в статье 986 ГК РУз: лицо, допустившее нарушение договора, несёт перед другой стороной договорную ответственность, а требования о возмещении вреда из деликта возможны лишь в случае, когда действиями должника причинён вред жизни, здоровью или имуществу, не охватываемый предметом договора.¹¹

В международных арбитражных отношениях конкуренция требований осложняется коллизионными вопросами: место нахождения арбитражного института, место обработки данных, место наступления вреда и место нахождения потерпевшего могут находиться в различных юрисдикциях. В подобных ситуациях применимое право определяется на основании коллизионных норм международного частного права каждой юрисдикции; при этом договорный статут, как правило, подчиняется праву, избранному сторонами, тогда как деликтный статут определяется по закону места причинения вреда (*lex loci delicti*) или наиболее тесной связи.

Регламенты ведущих арбитражных институтов - МТП, ЮНСИТРАЛ, МЦУИС как правило, содержат оговорки о применимом праве к административному договору, однако вопросы деликтной ответственности за нарушение кибербезопасности в действующих редакциях регламентов не урегулированы в явном виде.¹² Данный пробел требует восполнения путём включения в регламенты специальных положений о киберинцидентах, применимых стандартах безопасности и порядке уведомления сторон в случае нарушения защиты данных.

Доказывание ущерба и вопросы причинно-следственной связи. Одним из наиболее сложных аспектов гражданско-правовой ответственности арбитражных институтов за нарушения кибербезопасности является доказывание убытков и

¹⁰Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан. 2022. № 03/22/764/0278.

¹¹ICC Commission Report on Information Technology in International Arbitration. ICC Publication No. 963E. Paris: ICC Publishing, 2019. P. 12–45.

¹²Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 г. № 560-II (с изм. и доп.) // Ведомости Олий Мажлиса Республики Узбекистан. 2004. № 1–2. Ст. 10.

причинно-следственной связи. Ущерб, возникающий вследствие утечки конфиденциальной информации в ходе арбитражного разбирательства, может носить как имущественный, так и неимущественный характер. К имущественному ущербу относятся: раскрытие коммерческой тайны и утрата конкурентных преимуществ, несанкционированное использование стратегических позиций сторон третьими лицами, утечка сведений о доказательственной базе, а также расходы на устранение последствий киберинцидента. Неимущественный ущерб может выражаться в нарушении деловой репутации и подрыве доверия к арбитражной процедуре.

Установление причинно-следственной связи между нарушением кибербезопасности и конкретными убытками требует, как правило, проведения специализированной судебно-технической экспертизы. При этом суды (и трибуналы) нередко применяют стандарт «баланса вероятностей» (*more probable than not*) для установления того, что именно ненадлежащие меры безопасности арбитражного института стали причиной конкретного инцидента, а не внешние факторы, находившиеся вне его контроля. Данная проблематика соотносится с нормой статьи 14 ГК РУз о составе убытков, включающих реальный ущерб и упущенную выгоду.

Рекомендации по совершенствованию правового регулирования. На основании проведённого анализа можно сформулировать следующие рекомендации в области законодательного и институционального регулирования.

В законодательной сфере представляется необходимым: внести в Закон Республики Узбекистан «О международном коммерческом арбитраже» специальную статью об обязательствах арбитражных институтов по обеспечению кибербезопасности и ответственности за их нарушение; привести нормы Закона «О персональных данных» в полное соответствие с международными стандартами защиты данных применительно к деятельности арбитражных учреждений; закрепить в подзаконных актах минимальные требования к технической защите информационных систем арбитражных институтов по аналогии с европейской Директивой NIS 2.

В части совершенствования регламентной базы арбитражных учреждений рекомендуется: включить в регламенты арбитражных институтов (в том числе Ташкентского международного арбитражного центра) специальный раздел о кибербезопасности, предусматривающий стандарты защиты данных, процедуру уведомления о киберинцидентах и механизм возмещения ущерба; разграничить иммунитет арбитра (применительно к квазисудебным функциям) и ответственность института (применительно к административным и технологическим функциям); установить обязательное страхование профессиональной ответственности арбитражных институтов за киберриски.

Заключение. Гражданско-правовая ответственность арбитражных институтов за нарушения кибербезопасности представляет собой самостоятельный и недостаточно изученный институт на стыке деликтного, договорного и информационного права. Двойственный правовой статус арбитражного института порождает конкуренцию договорных и деликтных требований, разрешение которой зависит как от применимого национального права, так и от конкретных положений регламента.

Действующая нормативная база, включая законодательство Республики Узбекистан, не содержит специальных норм, адекватно регулирующих данную сферу, что создаёт правовую неопределённость для сторон арбитражных разбирательств.

Устранение выявленных пробелов требует комплексного подхода: обновления арбитражного законодательства, совершенствования регламентной базы арбитражных учреждений и гармонизации норм о защите данных с международными стандартами. Настоящее исследование обозначает проблему и определяет основные направления дальнейшей научной разработки вопросов ответственности арбитражных институтов в цифровую эпоху..

Список литературы:

1. Born G.B. International Commercial Arbitration (3rd ed.). Kluwer Law International, 2021.
2. Schreuer C., Malintoppi L., Reinisch A., Sinclair A. The ICSID Convention: A Commentary (2nd ed.). Cambridge University Press, 2009.
3. Prosser W.L., Keeton W.P. Prosser and Keeton on the Law of Torts (5th ed.). West Publishing, 1984.
4. UNCITRAL Notes on Organizing Arbitral Proceedings (3rd ed., 2016). United Nations. URL: <https://uncitral.un.org>
5. ICC Commission Report on Information Technology in International Arbitration. ICC Publication No. 963E. Paris: ICC Publishing, 2019.
6. Regulation (EU) 2016/679 (GDPR) // OJ L 119. 4.5.2016.
7. Directive (EU) 2016/1148 (NIS Directive) // OJ L 194. 19.7.2016.
8. Закон Республики Узбекистан «О международном коммерческом арбитраже» от 16 февраля 2021 г. № ЗРУ-674 // Национальная база данных законодательства Республики Узбекистан. 2021. № 03/21/674/0123.
9. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 г. № ЗРУ-547 // Собрание законодательства Республики Узбекистан. 2019. № 27. Ст. 634.
10. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 г. № 560-II // Ведомости Олий Мажлиса Республики Узбекистан. 2004. № 1–2. Ст. 10.
11. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан. 2022. № 03/22/764/0278.
12. Гражданский кодекс Республики Узбекистан от 29 августа 1996 г. (с изм. и доп. по сост. на 2025 г.).