

ЦИФРОВАЯ ИНФРАСТРУКТУРА МЕЖДУНАРОДНОГО АРБИТРАЖА И НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО О КИБЕРБЕЗОПАСНОСТИ: ТОЧКИ ПРАВОВОГО СОПРЯЖЕНИЯ НА ПРИМЕРЕ РЕСПУБЛИКИ УЗБЕКИСТАН

Кайбылдаева Бегаим Мухитовна

Независимый исследователь,

Ташкентский государственный юридический университет.

Э- почта: begaimkaibylldaeva@gmail.com

<https://doi.org/10.5281/zenodo.20271652>

Введение. Цифровая трансформация международного коммерческого арбитража приобрела необратимый характер. Пандемия COVID-19 резко ускорила внедрение технологий в арбитражный процесс: виртуальные слушания, электронный документооборот, облачные платформы управления делами и системы искусственного интеллекта для анализа доказательств стали неотъемлемой частью ведущих арбитражных учреждений Арбитражного суда МТП ICC, МЦУИС, Лондонского международного арбитражного суда (LCIA) и Сингапурского международного арбитражного центра (SIAC). По данным ICC, в 2022 году свыше 80% арбитражных слушаний в рамках Арбитражного суда МТП проводилось в дистанционном или гибридном формате.

Цифровизация арбитражного процесса порождает новые уязвимости: конфиденциальные материалы дел, показания свидетелей, правовые стратегии и коммерчески чувствительные доказательства перемещаются через международные информационные сети, подвергаясь угрозам перехвата, несанкционированного доступа и фальсификации. Осознание данных рисков побудило ведущие арбитражные институты разработать специализированные стандарты в области кибербезопасности, наиболее концептуально оформленным из которых является Протокол о кибербезопасности в международном арбитраже 2020 года.

Для Республики Узбекистан это пересечение цифровой арбитражной инфраструктуры и национального законодательства о кибербезопасности представляет особую актуальность. Страна одновременно развивает потенциал международного арбитража посредством Ташкентского международного арбитражного центра (ТМАЦ), учреждённого в 2018 году, и формирует национальную регуляторную систему в области кибербезопасности. Эти два процесса, протекая параллельно, не получили надлежащей законодательной координации, что порождает правовые пробелы и потенциальные коллизии, способные препятствовать эффективному функционированию цифровых арбитражных разбирательств с участием узбекских сторон. Настоящая работа посвящена анализу ключевых точек правового сопряжения между указанными системами и выработке рекомендаций по их устранению.

Цифровая инфраструктура современного международного арбитража: ключевые элементы и нормативное регулирование. Цифровая инфраструктура международного арбитража охватывает несколько взаимосвязанных уровней. Первый образуют системы электронной подачи документов и управления делами, функционирующие в ведущих учреждениях. МЦУИС ввёл обязательный электронный документооборот в обновлённых Арбитражных правилах 2022 года; Арбитражный суд МТП ICC использует

платформу NetCase для защищённого обмена процессуальными документами; SIAC располагает специализированной системой онлайн-подачи документов. Вторым уровнем составляют платформы для проведения виртуальных слушаний, работающие на основе зашифрованных протоколов передачи данных. Третий уровень включает облачные хранилища доказательств и иных материалов дела, управляемые посредством специализированных юридических платформ Relativity, Opus 2 и TrialDirector.

Нормативный ответ на вызовы кибербезопасности в цифровом арбитраже был сформирован прежде всего на институциональном уровне. Протокол о кибербезопасности в международном арбитраже 2020 года, разработанный совместно МТП ICC, ICCA и NYIAC, устанавливает принципы пропорциональности, непрерывной оценки рисков, управления доступом и реагирования на инциденты. Документ носит рекомендательный характер, однако формирует стандарт должной осмотрительности для арбитражных учреждений, трибуналов и представителей сторон.¹

Примечания по организации арбитражного разбирательства ЮНСИТРАЛ 2016 года содержат ряд рекомендаций относительно технических мер защиты при проведении слушаний в дистанционном формате, однако предшествовали масштабному цифровому переходу 2020-2022 годов и не содержат специальных механизмов обеспечения кибербезопасности.² Ни Типовой закон ЮНСИТРАЛ о международном коммерческом арбитраже (с поправками 2006 года), ни Нью-Йоркская конвенция 1958 года не содержат положений о кибербезопасности арбитражных данных, что оставляет регулирование данной сферы преимущественно на институциональном и договорном уровнях. Это создаёт правовую неопределённость в юрисдикциях, где национальное законодательство о кибербезопасности предъявляет обязательные требования к обработке данных.³

Нормативно-правовая база кибербезопасности Республики Узбекистан. Национальная система кибербезопасности Узбекистана сформировалась в ходе масштабных реформ цифровой экономики, активно реализуемых с 2016 года. Ключевым нормативным актом в данной сфере служит Закон «О персональных данных» от 2 июля 2019 года (№ ЗРУ-547), устанавливающий требования к сбору, обработке, хранению и трансграничной передаче персональных данных. Статья 22 данного Закона вводит принцип локализации данных: базы персональных данных граждан Узбекистана подлежат хранению на серверах, физически расположенных на территории страны.⁴

Институциональную основу кибербезопасности образует система, включающая Агентство по кибербезопасности Республики Узбекистан, созданное в 2021 году, Государственную инспекцию по надзору в области кибербезопасности и Центр реагирования на компьютерные инциденты UZ-CERT. На Агентство возложены функции нормативного регулирования, надзора за критической информационной

¹ICC, ICCA, NYIAC. (2020). Cybersecurity Protocol for International Arbitration. International Chamber of Commerce. <https://iccwbo.org>

²UNCITRAL. (2016). Notes on Organizing Arbitral Proceedings (3rd ed.). United Nations. <https://uncitral.un.org>

³Born, G. B. (2021). International commercial arbitration (3rd ed.). Kluwer Law International.

⁴Республика Узбекистан. (2019). Закон «О персональных данных» (№ ЗРУ-547 от 2 июля 2019 г.), ст. 22. Ведомости Олий Мажлиса.

инфраструктурой и координации реагирования на кибератаки. Концепция развития системы защиты информации и обеспечения кибербезопасности на 2021-2023 годы определила стратегические ориентиры: внедрение аттестации объектов информатизации, создание государственных стандартов шифрования и расширение перечня объектов критической информационной инфраструктуры.⁵

Вместе с тем действующее законодательство ориентировано преимущественно на государственные информационные системы и оставляет за рамками специального регулирования деятельность международных арбитражных учреждений и их цифровые платформы. Закон «Об электронной коммерции» 2015 года и подзаконные акты в сфере электронного документооборота лишь отчасти восполняют этот пробел, не охватывая специфику арбитражного производства. Совокупность перечисленных нормативных актов создаёт правовую среду, в которой использование иностранных цифровых платформ для арбитражного производства с участием узбекских сторон сопряжено с комплексом правовых неопределённостей.

Точки правового сопряжения: коллизии и пробелы. Сопоставительный анализ действующих нормативных актов позволяет выделить четыре ключевые точки правового сопряжения между цифровой инфраструктурой международного арбитража и узбекским законодательством о кибербезопасности.

Первая и наиболее значимая точка коллизии связана с требованием локализации данных. Статья 22 Закона «О персональных данных» предписывает хранение персональных данных граждан Узбекистана на серверах, расположенных на территории страны. Между тем международные арбитражные учреждения МЦУИС, Арбитражный суд МТП ICC, SIAC - хранят материалы дел на зарубежных серверах и облачных платформах в юрисдикции места нахождения учреждения. В деле с участием физического лица гражданина Узбекистана буквальное применение данного требования к арбитражным материалам создаёт коллизию с принципами институциональных регламентов, поскольку исключений для международного арбитражного производства в тексте Закона не предусмотрено.⁶

Вторая точка сопряжения обусловлена широкими государственными полномочиями по доступу к данным. Законодательство о кибербезопасности наделяет компетентные органы правом запрашивать информацию от операторов данных при наличии угроз национальной безопасности. Принцип конфиденциальности является одним из краеугольных камней международного арбитража: раскрытие материалов дела государственным органам без согласия сторон несовместимо с природой арбитражного производства. Данная коллизия аналогична той, с которой столкнулись иные государства, принявшие законодательство о широком государственном доступе к данным, в частности, США в контексте применения CLOUD Act к данным, хранящимся за рубежом.⁷

Третья точка сопряжения связана с регулированием криптографических средств. Ряд постсоветских государств сохраняет требования об обязательной сертификации

⁵Ташкентский международный арбитражный центр. (2023). Арбитражный регламент ТМАЦ. <https://tiac.uz>

⁶Blackaby, N., Partasides, C., Redfern, A., & Hunter, M. (2015). Redfern and Hunter on International Arbitration (6th ed.). Oxford University Press.

⁷Born, G. B. (2021). International commercial arbitration (3rd ed.). Kluwer Law International.

криптографических решений уполномоченными органами. Международные арбитражные платформы применяют собственные протоколы шифрования (TLS 1.3 и выше, AES-256), которые могут не иметь соответствующей национальной сертификации, создавая регуляторную неопределённость для узбекских участников арбитражного процесса.

Четвёртая точка сопряжения касается режима трансграничной передачи данных. Закон «О персональных данных» допускает трансграничную передачу при соблюдении ряда условий, в том числе наличия согласия субъекта или соответствующего международного договора. Применительно к арбитражным разбирательствам, где стороны не всегда заблаговременно осознают конкретные последствия передачи данных в иностранные системы, выполнение данного условия нередко носит проблематичный характер.⁸

Рекомендации по совершенствованию правового регулирования. По итогам проведённого анализа возможно сформулировать комплекс мер по устранению выявленных точек коллизий.

В законодательной сфере представляется целесообразным предусмотреть в Законе «О персональных данных» специальное изъятие из требований о локализации данных применительно к материалам международных арбитражных разбирательств по аналогии с подходами, реализованными в законодательстве Китая (статья 38 Закона о защите персональной информации 2021 года) и ОАЭ (Федеральный декрет-закон № 45 от 2021 года о защите персональных данных). Кроме того, необходимо привести Закон «О международном коммерческом арбитраже» 2006 года в соответствие с актуальными тенденциями цифровизации арбитражных форм и установить правовой режим признания электронных арбитражных документов.

В институциональном плане рекомендуется принять руководящие принципы ТМАЦ о применении Протокола о кибербезопасности в международном арбитраже 2020 года, создать механизм взаимодействия ТМАЦ с Агентством по кибербезопасности для урегулирования инцидентов, затрагивающих арбитражные данные, без нарушения конфиденциальности производства, а также обеспечить участие сотрудников ТМАЦ в международных программах по кибербезопасности арбитража под эгидой ICC и SIAC Academy.

На уровне международного сотрудничества Узбекистану целесообразно изучить возможность присоединения к Будапештской конвенции о киберпреступности, нормы которой обеспечивают согласованный подход к трансграничному реагированию на киберинциденты, а также активизировать работу по гармонизации требований к шифрованию с международными стандартами серии ISO/IEC 27000 применительно к арбитражным данным.

Заключение. Цифровая инфраструктура международного арбитража и национальное законодательство о кибербезопасности представляют собой динамично развивающиеся правовые системы, взаимодействие которых на уровне Республики Узбекистан остаётся недостаточно осмысленным и законодательно урегулированным.

⁸Республика Узбекистан. (2019). Закон «О персональных данных» (№ ЗРУ-547), ст. 24. Ведомости Олий Мажлиса.

Выявленные точки правового сопряжения требование локализации данных, государственные полномочия по доступу к информации, стандарты шифрования и режим трансграничной передачи данных не являются непреодолимыми. Международный опыт, прежде всего практика Сингапура и Абу-Даби (ADGM), свидетельствует о принципиальной возможности создания правовой архитектуры, обеспечивающей как национальный суверенитет над данными, так и полноценное функционирование цифрового международного арбитража.

Реализация предложенных мер потребует межведомственного взаимодействия Министерства юстиции, Агентства по кибербезопасности и Торгово-промышленной палаты Республики Узбекистан при методологическом содействии ЮНСИТРАЛ и ведущих арбитражных учреждений. Итогом должна стать последовательная и предсказуемая правовая среда, в которой ТМАЦ сможет претендовать на роль регионального арбитражного хаба с высокими стандартами защиты данных.

Настоящая работа не претендует на исчерпывающий анализ всего спектра рассматриваемых проблем. Перспективными направлениями дальнейших исследований представляются: сравнительный анализ режимов локализации данных и их влияния на арбитражную привлекательность юрисдикции; изучение практики применения Протокола о кибербезопасности 2020 года в азиатских арбитражных центрах; оценка правовых последствий использования технологий распределённого реестра и смарт-контрактов в арбитражном производстве с участием узбекских сторон.

Adabiyotlar, References, Литературы:

1. Born, G. B. (2021). International commercial arbitration (3rd ed.). Kluwer Law International.
2. Blackaby, N., Partasides, C., Redfern, A., & Hunter, M. (2015). Redfern and Hunter on International Arbitration (6th ed.). Oxford University Press.
3. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention, ETS No. 185). <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
4. ICC, ICCA, NYIAC. (2020). Cybersecurity Protocol for International Arbitration. International Chamber of Commerce. <https://iccwbo.org>
5. ICSID. (2022). ICSID Arbitration Rules (effective 1 July 2022). World Bank Group. <https://icsid.worldbank.org>
6. International Chamber of Commerce. (2023). ICC Dispute Resolution Statistics 2022. ICC Publications.
7. ISO/IEC 27001:2022. Information security management systems - Requirements. International Organization for Standardization.
8. Республика Узбекистан. (2015). Закон «Об электронной коммерции» (№ ЗРУ-385 от 29 апреля 2015 г.). Ведомости Олий Мажлиса.
9. Республика Узбекистан. (2019). Закон «О персональных данных» (№ ЗРУ-547 от 2 июля 2019 г.). Ведомости Олий Мажлиса.
10. Ташкентский международный арбитражный центр. (2023). Арбитражный регламент ТМАЦ. <https://tiac.uz>
11. UNCITRAL. (2016). Notes on Organizing Arbitral Proceedings (3rd ed.). United Nations. <https://uncitral.un.org>

12. United Nations Commission on International Trade Law. (2006). UNCITRAL Model Law on International Commercial Arbitration (as amended 2006). United Nations. https://uncitral.un.org/en/texts/arbitration/modellaw/commercial_arbitration