“ADOLAT”
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=377

2026-yil
7-son
iyul
ISSN 3093-8546



Гражданско-правовой статус арбитражной платформы как субъекта отношений по обеспечению кибербезопасности: проблемы квалификации и регулирования

Бегаим Кайбылдаева,
Ташкентского государственного юридического университет,
независимый исследователь
e-mail: begaimkaibyldaeva@gmail.com

Аннотация. Raqamli texnologiyalarning jadal rivojlanishi va onlayn arbitraj amaliyotining kengayishi arbitraj platformalarini kiberxavfsizlikni ta'minlashga oid munosabatlar ishtirokchilari sifatida huquqiy jihatdan baholash zaruratini yuzaga keltirmoqda. Ushbu maqolada arbitraj platformasining fuqarolik-huquqiy maqomi, uni fuqarolik-huquqiy munosabatlar subyekti sifatida kvalifikatsiya qilish muammolari hamda axborot xavfsizligi talablarini buzganlik uchun javobgarlik masalalari o‘rganiladi. O‘zbekiston Respublikasi qonunchiligi, xususan, Kiberxavfsizlik to‘g‘risidagi, Shaxsga doir ma'lumotlar to‘g‘risidagi va Xalqaro tijorat arbitraji to‘g‘risidagi qonunlar tahlili asosida huquqiy tartibga solishdagi muhim bo‘shliqlar aniqlanib, ularni bartaraf etish bo‘yicha chora-tadbirlar taklif etiladi.

Калит сўзлар. arbitraj platformasi, kiberxavfsizlik, fuqarolik-huquqiy maqom, shaxsiy ma‘lumotlar, raqamli arbitraj, axborot xavfsizligi, O‘zbekiston, fuqarolik huquqi, javobgarlik, huquqiy tartibga solish.

Аннотация. Стремительное развитие цифровых технологий и расширение практики онлайн-арбитража порождают острую необходимость в правовой квалификации арбитражных платформ как участников отношений по обеспечению кибербезопасности. В настоящей статье исследуются гражданско-правовой статус арбитражной платформы, проблемы её квалификации в качестве субъекта гражданских правоотношений, а также вопросы ответственности за нарушение требований информационной безопасности. На основе анализа законодательства Республики Узбекистан, прежде всего Закона о кибербезопасности, Закона о персональных данных и Закона о международном коммерческом арбитраже, выявляются существенные пробелы в правовом регулировании и предлагаются меры по их устранению.

Ключевые слова. арбитражная платформа, кибербезопасность, гражданско-правовой статус, персональные данные, цифровой арбитраж, информационная безопасность, Узбекистан, гражданское право,

ответственность, правовое регулирование.

Annotation. The rapid development of digital technologies and the growing practice of online arbitration create an urgent need for the legal qualification of arbitration platforms as participants in cybersecurity relations. This article examines the civil-legal status of an arbitration platform, the problems of its qualification as a subject of civil legal relations, and issues of liability for violations of information security requirements. Based on an analysis of the legislation of the Republic of Uzbekistan, primarily the Law on Cybersecurity, the Law on Personal Data, and the Law on International Commercial Arbitration, significant gaps in legal regulation are identified and measures to address them are proposed.

Keywords. arbitration platform, cybersecurity, civil-legal status, personal data, digital arbitration, information security, Uzbekistan, civil law, liability, legal regulation.

Введение. Стремительная цифровизация коммерческих отношений обусловила широкое распространение онлайн-платформ для разрешения споров. Арбитражная платформа, функционирующая в качестве технологической инфраструктуры для проведения арбитражных разбирательств в электронной форме, включая организацию видеоконференций, хранение процессуальных документов, обеспечение защищённого обмена информацией между участниками арбитражного процесса и управление делопроизводством, занимает всё более значимое место в системе международного коммерческого арбитража. Вместе с тем её гражданско-правовой статус и роль в отношениях по обеспечению кибербезопасности остаются недостаточно исследованными в юридической науке.

Арбитражные платформы аккумулируют значительные массивы конфиденциальных данных: коммерческую тайну, персональные данные сторон, доказательственные материалы, позиции сторон и решения арбитров. Компрометация этих сведений в результате кибератак способна нанести непоправимый ущерб как участникам конкретного спора, так и репутации арбитражного института в целом. Именно поэтому вопрос о правовом положении арбитражной платформы как субъекта отношений по обеспечению кибербезопасности приобретает принципиальное практическое значение.

Настоящая статья ставит перед собой три взаимосвязанные задачи. Во-первых, установить гражданско-правовой статус арбитражной платформы в системе действующего законодательства Республики Узбекистан. Во-вторых, выявить проблемы квалификации платформы как субъекта правоотношений в сфере кибербезопасности. В-третьих, обозначить пути совершенствования правового

регулирования с учётом международных стандартов и лучших практик.

Понятие и виды арбитражных платформ: гражданско-правовая характеристика. Под арбитражной платформой понимается программно-аппаратный комплекс, предоставляющий технологическую инфраструктуру для проведения арбитражных разбирательств в электронной форме. В зависимости от организационной модели платформа может являться структурным подразделением арбитражного института (встроенная платформа), самостоятельным юридическим лицом, оказывающим услуги арбитражным институтам на договорной основе (независимая платформа), либо программным обеспечением, разработанным третьим лицом и переданным в пользование арбитражному институту (платформа-лицензиат).

Гражданский кодекс Республики Узбекистан [1] не содержит специальных норм об арбитражных платформах. Их правовое положение как участников гражданских правоотношений определяется общими нормами о юридических лицах (глава 4 ГК РУз) и нормами об информационных услугах. Вопрос о том, является ли арбитражная платформа самостоятельным субъектом гражданских правоотношений либо лишь инструментом другого субъекта, носит принципиальный характер для целей установления ответственности за нарушение требований кибербезопасности.

Закон Республики Узбекистан «О международном коммерческом арбитраже» [2] не упоминает арбитражные платформы в числе субъектов арбитражного разбирательства. Статья 6 Закона называет лишь арбитражный институт, арбитров и стороны. Тем самым платформа как таковая не обладает процессуальным статусом в понимании Закона, однако может нести гражданско-правовую ответственность перед арбитражным институтом и сторонами в силу договорных отношений.

Арбитражная платформа как субъект отношений по обеспечению кибербезопасности. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года [3] устанавливает правовые основы обеспечения кибербезопасности в стране. Статья 4 названного Закона определяет субъектов отношений в сфере кибербезопасности: государственные органы, юридические лица и индивидуальные предприниматели, являющиеся операторами информационных систем, а также пользователи информационных систем. Арбитражная платформа, функционирующая как информационная система, подпадает под действие данной нормы в качестве оператора.

Оператор информационной системы несёт обязанности по защите обрабатываемых данных, предупреждению инцидентов кибербезопасности и их устранению, а также по уведомлению

уполномоченных органов в случае возникновения инцидентов (статьи 12–14 Закона о кибербезопасности). Эти обязанности носят публично-правовой характер, однако их ненадлежащее исполнение влечёт и гражданско-правовую ответственность перед лицами, чьи данные были скомпрометированы.

Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года [4] обязывает операторов персональных данных принимать организационные и технические меры для их защиты. Арбитражная платформа, обрабатывающая персональные данные участников разбирательства (стороны, арбитры, свидетели, представители), является оператором персональных данных в соответствии со статьёй 3 названного Закона. Следовательно, на неё в полной мере распространяются обязанности оператора, включая получение согласия субъекта данных, обеспечение конфиденциальности и применение соразмерных мер защиты. Постановление Кабинета Министров Республики Узбекистан от 5 октября 2022 года № 570 [5] детализирует уровни защищённости персональных данных при их обработке, что непосредственно применимо к технической инфраструктуре арбитражных платформ.

Закон Республики Узбекистан «Об электронной цифровой подписи» от 12 октября 2022 года [6] регулирует вопросы применения электронных документов и цифровых подписей. Использование электронных цифровых подписей в арбитражных разбирательствах, осуществляемых посредством платформы, порождает дополнительные требования к технической инфраструктуре платформы в части обеспечения юридически значимого документооборота.

Принципиальная проблема квалификации состоит в том, что арбитражная платформа одновременно выступает в нескольких правовых ролях. Как оператор информационной системы она несёт публично-правовые обязанности в сфере кибербезопасности. Как сторона договора с арбитражным институтом она несёт договорную ответственность за качество услуг. Как оператор персональных данных она несёт обязанности перед субъектами этих данных. Эти роли могут вступать в конкуренцию, в особенности при определении объёма ответственности за инциденты кибербезопасности, затрагивающие конфиденциальность арбитражного разбирательства.

Проблемы ответственности арбитражной платформы за нарушение требований кибербезопасности. Вопрос об ответственности арбитражной платформы за нарушение требований кибербезопасности является одним из наиболее сложных в практическом отношении. Действующее законодательство Республики Узбекистан не предусматривает специальных норм об ответственности операторов арбитражных платформ, что порождает необходимость

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

применения общих механизмов гражданско-правовой ответственности.

В соответствии с главой 57 Гражданского кодекса Республики Узбекистан [1] ответственность за причинение вреда наступает при наличии совокупности условий: противоправного деяния, вреда, причинно-следственной связи и вины. Применительно к кибератакам установление причинно-следственной связи представляет особую сложность, поскольку нарушение кибербезопасности нередко является результатом действий третьих лиц. Вместе с тем ненадлежащее выполнение оператором обязанностей по защите данных образует самостоятельное противоправное деяние, дающее потерпевшему право на возмещение убытков.

Договорная ответственность арбитражной платформы перед арбитражным институтом определяется условиями соответствующего договора об оказании услуг. В международной практике такие договоры, как правило, включают положения о стандартах безопасности, уровне доступности сервиса и порядке распределения ответственности в случае инцидента. Однако Закон Республики Узбекистан «О международном коммерческом арбитраже» [2] не обязывает арбитражные институты включать в договоры с платформами специальные положения о кибербезопасности, что является существенным пробелом.

Постановление Президента Республики Узбекистан от 31 мая 2023 года № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры» [7] закрепляет конкретные требования к операторам объектов критической информационной инфраструктуры в части организации системы защиты, уведомления об инцидентах и взаимодействия с уполномоченными органами. Несмотря на то что арбитражные платформы прямо не отнесены к объектам критической инфраструктуры, положения названного постановления могут применяться в качестве ориентира для установления стандарта должной осмотрительности при оценке поведения оператора платформы.

Постановление Президента Республики Узбекистан от 30 апреля 2025 года № ПП-153 [8] определило Министерство внутренних дел уполномоченным органом по внедрению единой практики в сфере борьбы с киберпреступлениями и координации деятельности всех ответственных государственных органов в данном направлении. Хотя указанный акт ориентирован прежде всего на правоохранительный аспект, он свидетельствует о последовательном усилении государственного подхода к противодействию цифровым угрозам, в контексте которого вопросы квалификации операторов арбитражных платформ приобретают новую актуальность.

Сравнительный анализ подходов к регулированию. Международная практика выработала различные подходы к правовому регулированию арбитражных платформ. Сингапурский международный арбитражный центр (SIAC) разработал детализированные протоколы кибербезопасности для онлайн-слушаний, устанавливающие технические требования к платформам, процедуры верификации участников и порядок реагирования на инциденты. Международная торговая палата в Руководящих принципах по кибербезопасности для виртуальных слушаний (2020) рекомендует арбитражным трибуналам принимать протоколы кибербезопасности в самом начале разбирательства, определяя используемую платформу, процедуры аутентификации и порядок реагирования на инциденты [9].

В государствах Европейского союза на арбитражные платформы, обрабатывающие персональные данные граждан, распространяются требования Общего регламента по защите данных (GDPR). Это влечёт необходимость назначения ответственного за защиту данных, проведения оценки воздействия обработки данных на права субъектов и внедрения технической и организационной защиты. Казахстанский опыт представляет особый интерес ввиду общих правовых традиций с Узбекистаном: Казахстанский международный арбитражный центр закрепил в своих процессуальных правилах положения об электронном документообороте и защите данных, однако всеобъемлющего специального законодательства об арбитражных платформах также принято не было.

Анализ международного опыта позволяет выделить две основные регуляторные модели. Первая, институциональная, предполагает, что требования к платформам формулируются на уровне регламентов арбитражных институтов и договорных отношений. Вторая, законодательная, предусматривает, что государство устанавливает нормативные требования к платформам непосредственно на уровне законодательства. Для Республики Узбекистан с учётом специфики правовой системы наиболее приемлемой представляется комбинированная модель, сочетающая базовые законодательные требования с детализацией на уровне регламентов арбитражных институтов.

Выявленные пробелы и предложения по совершенствованию законодательства. Проведённый анализ позволяет выявить следующие пробелы в действующем законодательстве Республики Узбекистан применительно к правовому статусу арбитражных платформ.

Во-первых, Закон о международном коммерческом арбитраже [2] не содержит определения арбитражной платформы и не относит её к числу субъектов отношений в сфере арбитражного разбирательства. Введение в текст Закона

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

понятия арбитражной платформы и базовых требований к её технической инфраструктуре с точки зрения кибербезопасности является необходимым условием формирования ясной правовой основы.

Во-вторых, Закон о кибербезопасности [3], признавая операторов информационных систем субъектами соответствующих отношений, не учитывает специфику платформ, обслуживающих конфиденциальные юридические разбирательства. Разработка специальных подзаконных требований к уровню защиты информационных систем арбитражных платформ по аналогии с Постановлением № ПП-167 [7] для объектов критической инфраструктуры позволила бы устранить этот пробел.

В-третьих, отсутствует нормативная связь между Законом о международном коммерческом арбитраже и Законом о персональных данных [4] применительно к арбитражным платформам. Необходима специальная норма, разъясняющая, что персональные данные, обрабатываемые в ходе арбитражного разбирательства посредством платформы, подлежат защите в соответствии с Законом о персональных данных, а арбитражный институт и оператор платформы являются совместными операторами данных.

В-четвёртых, необходимо законодательно закрепить обязанность арбитражных институтов, осуществляющих разбирательства в Республике Узбекистан, использовать только те платформы, которые соответствуют установленным требованиям кибербезопасности, и включать в договоры с платформами специальные положения о распределении ответственности и порядке уведомления о киберинцидентах.

В-пятых, Закон о международном коммерческом арбитраже следует дополнить общей нормой о конфиденциальности арбитражного разбирательства, распространяющейся на всех участников, включая операторов технологической инфраструктуры. Это устранило бы существенное расхождение между узбекским арбитражным законодательством и международными стандартами.

Заключение. Арбитражная платформа занимает особое место в системе субъектов отношений по обеспечению кибербезопасности: она одновременно является оператором информационной системы, оператором персональных данных и стороной договорных правоотношений с арбитражным институтом. Действующее законодательство Республики Узбекистан не содержит специальных норм, регулирующих правовой статус арбитражных платформ, что порождает существенную неопределённость в вопросах квалификации и ответственности.

Совершенствование правового регулирования в данной сфере требует комплексного подхода, сочетающего внесение изменений в Закон о международном коммерческом

арбитраже, разработку подзаконных актов на основе Закона о кибербезопасности и Закона о персональных данных, а также стимулирование арбитражных институтов к принятию детализированных протоколов кибербезопасности на уровне регламентов. Реализация предложенных мер будет способствовать повышению привлекательности Республики Узбекистан как места проведения международного коммерческого арбитража и приведению национального законодательства в соответствие с современными международными стандартами.

Список литературы:

1. Гражданский кодекс Республики Узбекистан (часть первая утверждена Законом РУз от 21 декабря 1995 года № 163-I, часть вторая — Законом РУз от 29 августа 1996 года № 256-I; с изм. и доп. по состоянию на 25 декабря 2025 года). https://lex.uz/acts/111181 (Civil Code of the Republic of Uzbekistan, Part One approved by Law No. 163-I of 21 December 1995, Part Two by Law No. 256-I of 29 August 1996, with amendments as of 25 December 2025.)

2. Закон Республики Узбекистан «О международном коммерческом арбитраже» от 16 февраля 2021 года № ЗРУ-674. https://lex.uz/docs/5294087 (Law of the Republic of Uzbekistan «On International Commercial Arbitration» No. ZRU-674 of 16 February 2021.)

3. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764. https://lex.uz/docs/6997403 (Law of the Republic of Uzbekistan «On Cybersecurity» No. ZRU-764 of 15 April 2022.)

4. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547 (с изм. и доп., в том числе от 26 марта 2026 года № ЗРУ-1125). https://lex.uz/docs/4396428 (Law of the Republic of Uzbekistan «On Personal Data» No. ZRU-547 of 2 July 2019, with amendments including ZRU-1125 of 26 March 2026.)

5. Постановление Кабинета Министров Республики Узбекистан «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных» от 5 октября 2022 года № 570. https://lex.uz/docs/6225469 (Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 570 of 5 October 2022 «On the Approval of Certain Regulatory Legal Acts in the Field of Personal Data Processing».)

6. Закон Республики Узбекистан «Об электронной цифровой подписи» от 12 октября 2022 года № ЗРУ-793 (вступил в силу 14 января 2023 года). https://lex.uz/docs/6234906 (Law of the Republic of Uzbekistan «On Electronic Digital Signature» No. ZRU-793 of 12 October 2022, entered into force 14 January 2023.)

7. Постановление Президента Республики Узбекистан «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» от

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

31 мая 2023 года № ПП-167. https://lex.uz/docs/6479197 (Presidential Decree of the Republic of Uzbekistan No. PP-167 of 31 May 2023 «On Additional Measures to Improve the Cybersecurity System for Critical Information Infrastructure Facilities of the Republic of Uzbekistan».)

8. Постановление Президента Республики Узбекистан «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий» от 30 апреля 2025 года № ПП-153. https://lex.uz/docs/7511168 (Presidential Decree of the Republic of Uzbekistan No. PP-153 of 30 April 2025 «On Measures Aimed at Further Strengthening Activities to Combat Crimes Committed Using Information Technologies».)

9. International Chamber of Commerce. ICC Cybersecurity Guidelines for Virtual Hearings. Paris: ICC, 2020. (International Chamber of Commerce. ICC Cybersecurity Guidelines for Virtual Hearings. Paris: ICC, 2020.)

10. UNCITRAL Technical Notes on Online Dispute Resolution. New York: United Nations, 2017. (UNCITRAL Technical Notes on Online Dispute Resolution. New York: United Nations, 2017.)

11. Regulation (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 (General Data Protection Regulation). Official Journal of the European Union, L 119/1. (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119/1.)

12. Snyder F. The effectiveness of European Community law: institutions, processes, tools and techniques. Modern Law Review. 1993. Vol. 56. No. 1. P. 19-54. (Snyder F. The effectiveness of European Community law: institutions, processes, tools and techniques. Modern Law Review. 1993. Vol. 56. No. 1. P. 19-54.)