МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ISO/IEC 27001) В СИСТЕМЕ ГРАЖДАНСКО-ПРАВОВОГО РЕГУЛИРОВАНИЯ МЕЖДУНАРОДНОГО КОММЕРЧЕСКОГО АРБИТРАЖА РЕСПУБЛИКИ УЗБЕКИСТАН

Кайбылдаева Бегаим Мухитовна
Независимый исследователь, Ташкентский государственный юридический университет
Эл. почта: begaimkaibyldaeva@gmail.com
https://doi.org/10.5281/zenodo.21837473

Введение. Цифровизация международного коммерческого арбитража, выразившаяся в переходе к электронному обмену документами, удаленным слушаниям и облачному хранению доказательственных материалов, поставила перед национальными правовыми системами задачу выработки объективного критерия должной осмотрительности участников арбитражного разбирательства в области защиты информации. Республика Узбекистан, последовательно интегрирующаяся в систему международного коммерческого арбитража после принятия Закона «О международном коммерческом арбитраже» от 16 февраля 2021 года № ЗРУ-674, разработанного на основе Типового закона ЮНСИТРАЛ, сталкивается с необходимостью согласования национального гражданско-правового регулирования с общепризнанными международными техническими стандартами информационной безопасности, важнейшим из которых является международный стандарт ISO/IEC 27001.

Настоящее исследование посвящено анализу правовой природы стандарта ISO/IEC 27001 и его функции в системе источников, формирующих гражданско-правовой стандарт разумной осмотрительности (должной заботливости) сторон, арбитров и администрирующих учреждений при разрешении споров посредством международного коммерческого арбитража с местом арбитража в Республике Узбекистан. Исследование опирается на действующее законодательство Республики Узбекистан, размещенное в Национальной базе данных законодательства (lex.uz), а также на международные правовые и технические инструменты, включая сам стандарт ISO/IEC 27001, Типовой закон ЮНСИТРАЛ о международном торговом арбитраже, Нью-Йоркскую конвенцию 1958 года и отраслевые протоколы международных арбитражных институтов.

Правовая природа стандарта ISO/IEC 27001 и его место в системе источников гражданско-правового регулирования. Международный стандарт ISO/IEC 27001:2022, изданный Международной организацией по стандартизации совместно с Международной электротехнической комиссией, устанавливает требования к созданию, внедрению, поддержанию и постоянному совершенствованию системы менеджмента информационной безопасности организации. Стандарт носит добровольный характер и сам по себе не порождает юридически обязательных последствий, однако его повсеместное применение, подтверждаемое десятками тысяч действующих сертификатов соответствия по всему миру, превращает его в устоявшийся обычай делового оборота в сфере защиты информации.

С точки зрения гражданского права, добровольный технический стандарт подобного рода способен выполнять функцию, аналогичную функции торгового

обыкновения или сложившейся деловой практики, то есть служить объективным критерием при определении содержания обязанности проявлять разумную заботливость (due diligence), возлагаемой на участника гражданского оборота законом или договором. Статья 14 Гражданского кодекса Республики Узбекистан (часть первая), утвержденного Законом от 21 декабря 1995 года № 163-I, закрепляет право лица, чье право нарушено, на полное возмещение причиненных убытков, что при отсутствии специального технического регламента предполагает установление объективного мерила надлежащего поведения обязанного лица. Именно эту роль применительно к информационной безопасности способен выполнять стандарт ISO/IEC 27001, поскольку он предлагает измеримые и общепризнанные критерии организационных и технических мер защиты информации, применимые для оценки того, действовал ли участник арбитражного разбирательства разумно и добросовестно при обращении с материалами дела.

Национальная нормативно-правовая база Республики Узбекистан. Национальное законодательство Республики Узбекистан в сфере информационной безопасности и международного коммерческого арбитража образует многоуровневую систему актов. Закон «О международном коммерческом арбитраже» от 16 февраля 2021 года № ЗРУ-674 определяет в статье 4 широкую сферу применения арбитражного соглашения в отношении договорных и внедоговорных коммерческих споров и вступил в силу 18 августа 2021 года, распространяясь на арбитражные разбирательства, начатые после этой даты. Закон не содержит специальных технических требований к защите электронных документов арбитражного дела, что делает необходимым обращение к иным отраслевым актам.

Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764 устанавливает в статье 16 права и обязанности субъектов кибербезопасности, в статье 18 предусматривает экспертизу на соответствие требованиям кибербезопасности, а в статье 19 регулирует сертификацию аппаратных, аппаратно-программных и программных средств, что создает институциональную основу, совместимую с логикой сертификации по стандарту ISO/IEC 27001. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547 возлагает на операторов и субъектов, обрабатывающих персональные данные, обязанность принимать организационные и технические меры защиты, соразмерные рискам обработки, что по своему содержанию соответствует риск-ориентированному подходу, заложенному в стандарте ISO/IEC 27001. Дополнительное значение имеют Закон «Об электронном документообороте» от 29 апреля 2004 года № 611-II, регулирующий защиту электронных документов при их обороте, и Закон «Об электронной цифровой подписи» от 12 октября 2022 года № ЗРУ-793, обеспечивающий целостность и подлинность электронных документов, включая документы, представляемые сторонами арбитражного разбирательства.

Международно-правовые инструменты, дополняющие стандарт ISO/IEC 27001. Взаимодействие стандарта ISO/IEC 27001 с гражданско-правовым регулированием международного коммерческого арбитража Республики Узбекистан не может рассматриваться изолированно от системы международных правовых инструментов, формирующих единообразную практику в этой области. Типовой закон

ЮНСИТРАЛ о международном торговом арбитраже 1985 года с поправками 2006 года, положенный в основу Закона Республики Узбекистан «О международном коммерческом арбитраже», сам по себе не регулирует вопросы информационной безопасности, однако закрепленный им принцип автономии воли сторон позволяет включать технические стандарты, подобные ISO/IEC 27001, непосредственно в процедурные соглашения сторон и акты арбитражного учреждения.

Протокол по кибербезопасности для международного арбитража, разработанный Международным советом по коммерческому арбитражу (ICCA) совместно с Ассоциацией адвокатов города Нью-Йорка и Международным институтом по предотвращению и разрешению конфликтов (CPR), прямо ссылается на стандарт ISO/IEC 27001 в качестве иллюстративного ориентира для определения базовых практик информационной безопасности, не придавая ему при этом обязательной силы. Регламент Европейского Союза 2016/679 (Общий регламент по защите данных, GDPR) устанавливает обязанность оператора персональных данных применять надлежащие технические и организационные меры защиты и рассматривает соответствие признанным международным стандартам, включая ISO/IEC 27001, в качестве одного из доказательств исполнения этой обязанности. Признание арбитражных решений и приведение их в исполнение в иностранных государствах, включая государства-участники Нью-Йоркской конвенции о признании и приведении в исполнение иностранных арбитражных решений 1958 года, участницей которой является Республика Узбекистан, также предполагает, что процедура разбирательства, включая обращение с электронными доказательствами, отвечала общепризнанным международным стандартам добросовестности и надлежащей правовой процедуры.

Гражданско-правовой стандарт разумности и его соотношение с требованиями ISO/IEC 27001. Центральным элементом гражданско-правового анализа выступает соотношение между абстрактным требованием разумности и добросовестности, закрепленным в общих началах гражданского законодательства Республики Узбекистан, и конкретизированными техническими требованиями стандарта ISO/IEC 27001. Абстрактная формула разумного поведения, применяемая судами и арбитражными трибуналами при оценке ответственности за ненадлежащее обращение с конфиденциальной информацией, нуждается в объективном наполнении, которое стандарт ISO/IEC 27001 способен обеспечить посредством детализированного перечня организационных и технических мер контроля, содержащегося в приложении к стандарту.

Соответствие субъекта арбитражного разбирательства требованиям стандарта ISO/IEC 27001 не создает автоматической презумпции отсутствия вины в случае утраты или несанкционированного разглашения конфиденциальной информации, поскольку сам стандарт, как и упомянутый выше Протокол ICCA-NYC Bar-CPR, не устанавливает и не заменяет собой правила гражданско-правовой ответственности, определяемые применимым материальным правом. Вместе с тем демонстрируемое соответствие стандарту может служить относимым и допустимым доказательством разумности и добросовестности поведения соответствующего лица при распределении бремени доказывания вины по правилам, аналогичным содержащимся в статье 14 Гражданского

кодекса Республики Узбекистан, тогда как отклонение от общепризнанных требований стандарта способно свидетельствовать о непроявлении должной заботливости.

Проблемы применения ISO/IEC 27001 в узбекистанской арбитражной практике. Применение международного стандарта ISO/IEC 27001 в рамках гражданско-правового регулирования международного коммерческого арбитража Республики Узбекистан сталкивается с рядом трудностей. Во-первых, национальное законодательство не содержит прямой отсылочной нормы, связывающей исполнение обязанностей по обеспечению информационной безопасности участников арбитражного разбирательства с конкретным международным техническим стандартом, что оставляет определение применимого уровня защиты на усмотрение сторон и арбитражного трибунала в каждом конкретном деле.

Во-вторых, Ташкентский международный арбитражный центр при Торгово-промышленной палате Республики Узбекистан, образованный постановлением Президента Республики Узбекистан от 5 ноября 2018 года в качестве ведущего национального институционального арбитражного учреждения, не располагает собственным регламентом или процедурными правилами, детально регулирующими вопросы информационной безопасности по аналогии с протоколами ведущих зарубежных арбитражных институтов, что создает правовую неопределенность для сторон, планирующих арбитражное разбирательство на территории Республики Узбекистан. В-третьих, различие между добровольным характером сертификации по стандарту ISO/IEC 27001 и императивным характером требований Закона «О кибербезопасности» и Закона «О персональных данных» порождает необходимость дополнительного толкования вопроса о том, в какой мере соответствие добровольному международному стандарту освобождает субъекта от ответственности за нарушение императивных требований национального законодательства.

Рекомендации по совершенствованию законодательства. На основании проведенного анализа предлагается внесение в Закон Республики Узбекистан «О международном коммерческом арбитраже» дополнения, прямо предусматривающего право сторон и арбитражного трибунала согласовывать применение признанных международных стандартов информационной безопасности, включая ISO/IEC 27001, в качестве критерия оценки разумности мер защиты конфиденциальной информации арбитражного разбирательства. Целесообразным представляется также разработка Ташкентским международным арбитражным центром отдельного процедурного руководства (протокола) по вопросам информационной безопасности, учитывающего опыт Протокола ICCA-NYC Bar-CPR и содержащего прямую ссылку на международный стандарт ISO/IEC 27001 в качестве базового ориентира.

Дополнительно рекомендуется уточнить соотношение Закона «О кибербезопасности» и Закона «О персональных данных» с добровольными международными стандартами путем законодательного закрепления правила, согласно которому документально подтвержденное соответствие субъекта арбитражного разбирательства требованиям стандарта ISO/IEC 27001 учитывается судом или арбитражным трибуналом в качестве доказательства принятия разумных и достаточных мер защиты информации при разрешении споров о гражданско-правовой ответственности за нарушение конфиденциальности.

Заключение. Международный стандарт ISO/IEC 27001, не обладая самостоятельной юридической силой, тем не менее выполняет значимую функцию в системе гражданско-правового регулирования международного коммерческого арбитража Республики Узбекистан, предоставляя объективное содержательное наполнение абстрактного требования разумности и должной заботливости, закрепленного в статье 14 Гражданского кодекса Республики Узбекистан и производного от него законодательства о кибербезопасности, персональных данных и электронном документообороте.

Интеграция ссылок на данный стандарт в Закон «О международном коммерческом арбитраже» и в процедурные акты Ташкентского международного арбитражного центра, наряду с учетом положений Типового закона ЮНСИТРАЛ, Нью-Йоркской конвенции 1958 года и специализированных протоколов международных арбитражных институтов, способна повысить предсказуемость гражданско-правовой ответственности за нарушение информационной безопасности и укрепить позиции Республики Узбекистан как привлекательного места проведения международного коммерческого арбитража.

Adabiyotlar, References, Литературы:

1. Гражданский кодекс Республики Узбекистан (часть первая), утвержден Законом Республики Узбекистан от 21 декабря 1995 года № 163-I (с изменениями и дополнениями). https://lex.uz/docs/111181
2. Гражданский кодекс Республики Узбекистан (часть вторая), утвержден Законом Республики Узбекистан от 29 августа 1996 года (с изменениями и дополнениями). https://lex.uz/docs/180550
3. Европейский Парламент и Совет Европейского Союза. (2016). Регламент (ЕС) 2016/679 о защите физических лиц при обработке персональных данных (Общий регламент по защите данных, GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj
4. Закон Республики Узбекистан «О международном коммерческом арбитраже» от 16 февраля 2021 года № ЗРУ-674. https://lex.uz/docs/5294087
5. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764 (с изменениями и дополнениями). https://lex.uz/ru/docs/5960609
6. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547 (с изменениями и дополнениями). https://lex.uz/docs/4396428
7. Закон Республики Узбекистан «Об электронном документообороте» от 29 апреля 2004 года № 611-II (с изменениями и дополнениями). https://lex.uz/docs/165074
8. Закон Республики Узбекистан «Об электронной цифровой подписи» от 12 октября 2022 года № ЗРУ-793. https://lex.uz/ru/docs/6234906
9. Закон Республики Узбекистан «Об информатизации» (с изменениями и дополнениями). https://lex.uz/acts/82956
10. ICCA, New York City Bar Association, CPR. (2022). Протокол по кибербезопасности для международного арбитража (2022 Edition). CPR Dispute Resolution Services. https://drs.cpradr.org/rules/protocols-guidelines/icca-nyc-bar-cybersecurities
11. International Organization for Standardization, International Electrotechnical Commission. (2022). ISO/IEC 27001:2022, Information security, cybersecurity and privacy

protection, Information security management systems, Requirements. https://www.iso.org/standard/27001

12. Конвенция Организации Объединенных Наций о признании и приведении в исполнение иностранных арбитражных решений (Нью-Йоркская конвенция), 1958 год. https://uncitral.un.org/ru/texts/arbitration/conventions/foreign_arbitral_awards

13. Типовой закон ЮНСИТРАЛ о международном торговом арбитраже 1985 года с изменениями, принятыми в 2006 году. Комиссия Организации Объединенных Наций по праву международной торговли

14. Постановление Президента Республики Узбекистан от 5 ноября 2018 года о создании Ташкентского международного арбитражного центра при Торгово-промышленной палате Республики Узбекистан.