ЎЗБЕКИСТОН ҚОНУНЧИЛИГИ ТАҲЛИЛИ

UZBEKISTAN LAW REVIEW

ОБЗОР ЗАКОНОДАТЕЛЬСТВА УЗБЕКИСТАНА

ИЛМИЙ ТАҲЛИЛИЙ ЖУРНАЛ	SCIENTIFIC ANALYTICAL JOURNAL	НАУЧНО АНАЛИТИЧЕСКИЙ ЖУРНАЛ

2024

№4

Маълумот олиш учун қуйидагиларга мурожаат этиш сўралади:
Гулямов Саид Саидахрарович,
Рустамбеков Исламбек Рустамбекович
ТДЮУ, Халқаро хусусий ҳуқуқ кафедраси,
Ўзбекистон Республикаси, Тошкент ш., 100047,
Сайилгоҳ кўчаси, 35. Тел: 233-66-36

"Ўзбекистон қонунчилиги таҳлили"нинг электрон нусхаси Интернетдаги www.library-tsul.uz ёки www.lawreview.uz сайтида жойлаштирилган.

Журнал 2013 йилдан Ўзбекистон Республикаси Вазирлар Маҳкамасининг Олий Аттестация комиссияси журналлари рўйхатига киритилган.

2024 йилда нашр этилди.

ISSN 2181-8118

Масъул котиб: **И. Рустамбеков**
Нашриёт муҳаррири: **Н. Ниязова**
Техник муҳаррир: **Д. Козимов**
Лицензия № 02-0074
Босишга рухсат этилди – 25.12.2024
Нашриёт ҳисоб табоғи – 5
«IMPRESS MEDIA» босмахонасида босилди
Адади – 100 нусха.

ИЛМИЙ-ТАҲЛИЛИЙ ЖУРНАЛ

4/2024

МУНДАРИЖА

Саидов Баходирхужа Носирхужаевич
Ведущий специалист Центра кибербезопасности Главного управления устрашения Национальной гвардии Республики Узбекистан

ПРОБЛЕМЫ ГРАЖДАНСКО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ОХРАНЯЕМЫХ ОБЪЕКТОВ: ДОГОВОРНЫЕ АСПЕКТЫ

Аннотация. В эпоху цифровой трансформации охраняемые объекты, включающие здания, сооружения, транспортные средства и иные критически важные объекты, сталкиваются с новыми вызовами в сфере кибербезопасности. Взаимодействие физических и цифровых аспектов охраны требует эффективных гражданско-правовых механизмов регулирования. В данной работе рассматриваются договорные аспекты обеспечения кибербезопасности охраняемых объектов в Узбекистане, анализируются существующие правовые механизмы, выявляются пробелы и предлагаются рекомендации по совершенствованию законодательства и договорных отношений. Основное внимание уделяется договорам с провайдерами кибербезопасности, вопросам ответственности и распределения рисков, а также международному опыту регулирования киберугроз.

Ключевые слова: кибербезопасность, охраняемые объекты, договорное регулирование, гражданско-правовая ответственность, цифровые риски, законодательство Узбекистана, защита информации.

Annotatsiya. Raqamli transformatsiya davrida himoyalangan ob'ektlar, jumladan, binolar, inshootlar, transport vositalari va boshqa muhim ob'ektlar kiberxavfsizlik sohasida yangi muammolarga duch kelmoqda. Xavfsizlikning jismoniy va raqamli jihatlarining o'zaro ta'siri fuqarolik-huquqiy tartibga solishning samarali mexanizmlarini talab qiladi. Ushbu maqolada O‘zbekistonda qo‘riqlanadigan obyektlarning kiberxavfsizligini ta’minlashning shartnomaviy jihatlari ko‘rib chiqiladi, mavjud huquqiy mexanizmlar tahlil qilinadi, kamchiliklar aniqlanadi va qonunchilik va shartnomaviy munosabatlarni takomillashtirish bo‘yicha tavsiyalar beriladi. Asosiy e’tibor kiberxavfsizlik provayderlari bilan tuzilgan shartnomalar, javobgarlik va xavflarni taqsimlash masalalari hamda kibertahdidlarni tartibga solish bo‘yicha xalqaro tajribaga qaratiladi.

Kalit so‘zlar: kiberxavfsizlik, himoyalangan ob’ektlar, shartnomaviy tartibga solish, fuqarolik javobgarligi, raqamli risklar, O'zbekiston qonunchiligi, axborotni himoya qilish.

Abstract. In the era of digital transformation, protected objects, including buildings, structures, vehicles and other critical objects, face new challenges in the field of cybersecurity. The interaction of physical and digital aspects of security requires effective civil-legal regulatory mechanisms. This paper examines the contractual aspects of ensuring cybersecurity of protected objects in Uzbekistan, analyzes existing legal mechanisms, identifies gaps and offers recommendations for improving legislation and contractual relations. The main attention is paid to contracts with cybersecurity providers, issues of liability and risk allocation, as well as international experience in regulating cyber threats.

Keywords: cybersecurity, protected objects, contractual regulation, civil liability, digital risks, legislation of Uzbekistan, information protection.

Введение

В эпоху цифровой трансформации даже традиционные охраняемые объекты – здания, сооружения, транспортные средства, ценные грузы и т.д. – сталкиваются с новыми вызовами кибербезопасности. Под охраняемыми объектами Закон Узбекистана понимает материальные ценности или лица, принятые под охрану в установленном порядке. Их правовая природа сводится к объектам права собственности либо личным нематериальным благам (жизнь и здоровье охраняемого лица), требующим защиты. В цифровую эпоху значимость этих объектов возросла: они часто включают информационные системы (например, системы видеонаблюдения, контроллеры доступа, сети связи), которые сами нуждаются в защите от кибератак. Следовательно, кибербезопасность охраняемых объектов становится неотъемлемой частью их охраны, требуя гражданско-правовых механизмов для надлежащего регулирования.

В данном тезисе рассматриваются проблемы договорного обеспечения кибербезопасности охраняемых объектов. Будут раскрыты правовая природа этих объектов, существующие договорные механизмы киберзащиты (обязательства сторон, соглашения с IT-компаниями и провайдерами безопасности), анализ законодательства Узбекистана, пробелы и недостатки правового регулирования, вопросы гражданско-правовой ответственности за киберинциденты, а также представлены рекомендации по совершенствованию договорных отношений в сфере кибербезопасности.

Правовая природа охраняемых объектов и их значимость в цифровую эпоху

Охраняемые объекты в традиционном понимании – это материальные объекты или лица, находящиеся под физической защитой. Закон Республики Узбекистан "Об охранной деятельности" (ЗРУ-778 от 15.06.2022) дает широкое определение: охраняемый объект – здания, сооружения, транспортные средства, грузы, денежные средства, материальные ценности, а также физическое лицо, принятые под охрану. Правовая природа этих объектов заключается в том, что они являются объектами гражданских прав (имущество или личные блага), обладающими признаками неприкосновенности, охрана которых обеспечивается дого-

вором или законом.

В цифровую эпоху охраняемые объекты обрастают информационными системами: система сигнализации, камеры с IP-сетью, базы данных пропусков и пр. Таким образом, возникает двойственная природа охраняемого объекта – физическая и цифровая. Значимость этих объектов резко возросла, поскольку кибератака на них может привести к тем же или большим последствиям, что и физическое посягательство. Например, взлом информационной системы охраняемого объекта способен отключить сигнализацию или получить данные о передвижениях, что создаёт угрозу безопасности. Поэтому обеспечение кибербезопасности становится критически важным компонентом охраны. Государство Узбекистан, осознавая эти вызовы, в 2022 году приняло первый Закон "О кибербезопасности" (№ ЗРУ-764 от 15.04.2022), направленный на защиту критических объектов инфраструктуры и информационных систем. Этот закон устанавливает требования к обеспечению кибербезопасности информационных систем, особенно в секторах, отнесённых к критической инфраструктуре (оборона, энергетика, банковский сектор и др.) . Хотя охраняемые объекты не всегда равны критической инфраструктуре, многие из них (банки, стратегические предприятия) подпадают под эти категории, что подчёркивает их значимость и необходимость правовой защиты в киберсфере.

Таким образом, правовая природа охраняемых объектов сегодня включает не только физический аспект, но и цифровой. Их значимость обусловлена потенциальным ущербом от киберинцидентов: утрата конфиденциальных данных, остановка работы объектов, угрозы жизни и имуществу. Гражданско-правовое регулирование должно адекватно отражать эту двойственную природу, обеспечивая защиту как от физических, так и от киберугроз.

Договорные механизмы обеспечения кибербезопасности охраняемых объектов

Договор является ключевым инструментом гражданско-правового обеспечения кибербезопасности. В контексте охраняемых объектов можно выделить несколько видов договорных отношений, направленных на их защиту в киберпространстве:

•Договоры с провайдерами кибербезопасности. Владельцы или операторы охраняемых объектов часто привлекают внешних специализированных лиц (IT-компании, провайдеры услуг информационной безопасности, MSSP – Managed Security Service Providers) для защиты своих информационных систем. Такие договоры обычно относятся к возмездному оказанию услуг или подрядным, предметом которых являются услуги киберзащиты (мониторинг сетей, реагирование на инциденты, аудит безопасности, установка и обслуживание систем защиты). В договорах детально прописываются обязательства сторон: провайдер обязан обеспечить определённый уровень защиты, реагировать на инциденты в установленные сроки, хранить конфиденциальность данных, уведомлять о пробелах и атаках; заказчик обязан предоставлять необходимый доступ к системам, соблюдать рекомендации по безопасности, своевременно оплачивать услуги. Практика выработала Service-Level Agreements (SLA) – соглашения об уровне сервиса, которые являются приложениями к таким договорам. SLA определяет ожидаемый уровень услуг, время реакции на инциденты, допустимые простои системы и пр., устанавливая тем самым параметры ответственности в случае нарушений. Например, договор может предусматривать, что провайдер должен оповестить заказчика о выявленном киберинциденте незамедлительно, но не позднее, скажем, 24 часов, и начать меры по устранению последствий. Невыполнение этого условия рассматривается как существенное нарушение договора. Аналогично, внедрение и поддержка плана реагирования на инциденты может быть обязательством провайдера.

•Договоры на техническую охрану с элементами ИТ. Традиционные охранные предприятия, обеспечивающие физическую защиту объектов, все чаще включают в свои услуги и техническую защиту (сигнализация, видеонаблюдение, контроль доступа). В договорах охраны теперь появились разделы о кибербезопасности: например, обязательство охранной организации защищать каналы связи сигнализации от взлома, обеспечивать шифрование данных с камер, поддерживать актуальность программного обеспечения. Если охранная компания привлекает субподрядчиков-IT для этих целей, то составляются соответствующие трехсторонние соглашения или отдельные договоры субподряда, в которых распределяются задачи по киберзащите.

•Договоры на программное обеспечение и оборудование безопасности. Охраняемые объекты часто оснащаются программно-аппаратными комплексами безопасности (например, система управления доступом, пожарно-охранная сигнализация с сетевым подключением). Договоры поставки и обслуживания такого оборудования включают условия кибербезопасности: обновление прошивок, устранение уязвимостей, сертификация средств защиты. Закон "О кибербезопасности" Узбекистана требует сертифицировать аппаратное и программное обеспечение, используемое на критических объектах, что должно отражаться в договорах с поставщиками техники.

Важным элементом всех этих договорных механизмов являются положения об ответственности и распределении рисков. Как правило, стороны стремятся заранее определить, кто и в каком объёме несёт убытки в случае киберинцидента. Например, индемнити и ограничение ответственности: контракт может содержать обязанность провайдера возместить убытки, причинённые утечкой данных по его вине, а также ограничение – например, верхний предел ответственности равен сумме договора или определённой фиксированной сумме . Такой ограничительный оговор (limitation of liability) защищает исполнителя от чрезмерных финансовых рисков, но одновременно остав-

ляет заказчику определённую гарантированную компенсацию. Кроме того, рекомендуемой практикой является наличие у провайдера страхования профессиональной ответственности или киберстрахования, которое покроет ущерб от инцидентов . В договорах могут быть условия о страховании: провайдер гарантирует, что застраховал свою ответственность, или стороны договариваются совместно приобретать страховой полис на случай киберинцидентов.

Также договорные механизмы включают обязательства по конфиденциальности и защите данных (NDA, соглашения о неразглашении) – они обеспечивают, что информация об уязвимостях объекта, персональные данные и иная чувствительная информация, к которой получает доступ подрядчик, будут защищены и не попадут к третьим лицам. Нарушение таких условий влечёт как договорную ответственность, так и административные санкции согласно Закону "О персональных данных" (например, штрафы за незаконное распространение персональных данных).

Итак, на практике уже используются разнообразные договорные механизмы для обеспечения кибербезопасности охраняемых объектов. Однако эффективность их применения зависит от качества правового регулирования и осведомлённости сторон.

Законодательство Узбекистана: состояние, пробелы и недостатки

Действующее законодательство Узбекистана затрагивает вопросы кибербезопасности и охраны объектов фрагментарно, оставляя ряд пробелов в договорном регулировании:

•Закон "О кибербезопасности" (2022) – первый комплексный акт в этой сфере. Он устанавливает обязанности операторов объектов критической информационной инфраструктуры по обеспечению кибербезопасности . В частности, операторы обязаны соблюдать требования регулятора, обеспечивать непрерывную работу систем, хранить резервные копии данных, устанавливать системы мониторинга атак, сертифицировать оборудование и ПО, уведомлять о киберинцидентах и сотрудничать с госорганами в расследовании. Эти нормы напрямую адресованы организациям, владеющим критическими объектами (госпредприятия, банки, энергетика и др.), и носят императивный характер, не опосредованные договором. Однако закон не раскрывает, как именно эти требования должны исполняться во взаимоотношениях с подрядчиками или провайдерами услуг. То есть, он не регламентирует типовые условия договоров с IT-компаниями, а лишь говорит об обязанностях операторов перед государством. В результате остается пробел: когда оператор привлекает частную фирму для киберзащиты, их отношения строятся только на общих нормах гражданского права, без специальных указаний закона о кибербезопасности.

•Закон "Об охранной деятельности" (2022) – регулирует охрану объектов, но акцентирован на физической охране. В нем отсутствуют упоминания о кибербезопасности. Охрана определяется как деятельность по защите охраняемых объектов от посягательств и обеспечению режимов на объекте. Субъекты охранной деятельности – Национальная гвардия, МВД, Минобороны (на договорной основе), а также частные охранные организации (видимо, в законе отдельно не упомянуты, но подразумеваются под обращениями юрлиц). Закон регламентирует вопросы лицензирования охранных услуг, применение силы, права и обязанности охранников. Однако кибернетические аспекты защиты объектов (например, охрана информационных систем объекта от удалённого доступа) не отражены. Это существенный недостаток: современные охранные компании фактически сталкиваются с киберрисками (например, злоумышленник может попытаться отключить сигнализацию через интернет), но законодательно их обязанности на этот счёт не прописаны. Пробел влияет и на договоры: типовой договор охраны по узбекскому законодательству может не включать условий о кибербезопасности, если стороны сами не позаботятся об этом.

•Закон "Об информатизации" (2003) и связанные акты в сфере информационной безопасности. Закон об информатизации устарел и не учитывает современных реалий киберугроз. Он закрепляет общие принципы использования информационных систем и распределение полномочий госорганов. Специальных норм о договорах в сфере кибербезопасности там нет. Аналогично, нормативные акты о защите информации, принятые ранее (например, постановления правительства о технической защите информации), не адаптированы под гражданско-правовое регулирование киберуслуг.

•Закон "О персональных данных" (2019) – устанавливает требования к безопасности обработки персональных данных (конфиденциальность, предотвращение несанкционированного доступа). Для охраняемых объектов это актуально, если они обрабатывают персональные данные (например, данные посетителей, сотрудников). Закон обязывает оператора данных принимать организационные и технические меры защиты. Нарушение ведёт к административной и даже уголовной ответственности. Однако гражданско-правовая ответственность в этом законе прямо не прописана – пострадавшие лица теоретически могут требовать компенсации морального вреда или имущественного ущерба на основании общих норм Гражданского кодекса, но специальных механизмов (например, коллективных исков за утечку данных) узбекское право пока не предусматривает. Для договорной темы это значит, что в контрактах с IT-провайдерами обязательно должны быть условия о соблюдении требований Закона о персональных данных, иначе заказчик (оператор) рискует получить штраф от государства, но не иметь регресса к провайдеру.

•Гражданский кодекс Узбекистана – общий фундамент для договорных отношений и ответственности. Он применим ко всем ситуациям, не урегулированным

специальными законами. В контексте кибербезопасности ГК пока не содержит специальных норм. Ответственность подрядчика или исполнителя услуг за некачественное выполнение (ст. 359, 983 ГК и др.) распространяется и на услуги по кибербезопасности. Однако особенность киберуслуг – нематериальный результат и вероятностный характер (невозможно гарантировать абсолютную защиту). В правоприменении это может осложнять доказательство вины и причинно-следственной связи. Например, если охранная фирма обеспечивала кибербезопасность объекта, но произошёл взлом, нужно доказать, что именно неисполнение договорных обязанностей (например, неустановка обновления) привело к взлому, что может требовать технической экспертизы. ГК Узбекистана не содержит специальных презумпций или облегчений доказывания для таких случаев, что можно считать регулятивным пробелом.

Подводя итог анализу: законодательство Узбекистана в сфере договорного обеспечения кибербезопасности охраняемых объектов ещё формируется. Закон о кибербезопасности ввёл общие рамки, но не детализировал частноправовые аспекты. Закон об охране игнорирует киберугрозы. Закон о персональных данных фокусируется на публично-правовых санкциях. Отсюда возникают недостатки: отсутствие стандартов типовых договоров, неясность требований к частным провайдерам, слабая определённость гражданско-правовой ответственности. Эти пробелы снижают эффективность защиты, так как стороны могут не предусмотреть важных условий, а пострадавшие – столкнуться с трудностями взыскания ущерба.

Гражданско-правовая ответственность за киберинциденты охраняемых объектов

Киберинцидент – событие в киберпространстве, приводящее к нарушению работы информационных систем или утечке информации. В контексте охраняемых объектов киберинцидентами могут быть: взлом системы безопасности здания, кража данных посетителей, отключение автоматизированных систем управления (например, на производственном объекте) и т.п. Возникает вопрос: кто и в каком порядке несёт гражданско-правовую ответственность за последствия таких инцидентов?

Возможны различные ситуации ответственности:

•Ответственность по договору. Если между собственником (оператором) охраняемого объекта и компанией, оказывающей услуги кибербезопасности, заключён договор, то при наступлении инцидента анализируют, не нарушил ли исполнитель условия договора. Например, провайдер мог обязаться поддерживать актуальные средства защиты, но не обновил критическое программное обеспечение, что позволило хакеру проникнуть в сеть. Это будет рассматриваться как неисполнение (ненадлежащее исполнение) обязательства, и заказчик вправе требовать возмещения причинённых таким нарушением убытков (ст. 21, 985 ГК РУз). Убытки могут включать прямой имущественный ущерб (стоимость восстановления систем, простой в работе) и упущенную выгоду (например, потеря прибыли из-за простоя). Однако на практике исполнители часто ограничивают свою ответственность в договоре, как отмечалось ранее. Например, договором может быть предусмотрено, что провайдер не отвечает за косвенные убытки или что максимальная сумма ответственности – определённый лимит .

Гражданское право Узбекистана в целом допускает соглашения об ограничении ответственности, кроме случаев умысла или грубой неосторожности исполнителя. Поэтому в случае грубой небрежности (например, полное отсутствие обещанных мер защиты) суд мог бы признать недействительным слишком низкий лимит ответственности. Но эти вопросы ещё не обкатаны судебной практикой, что создаёт правовую неопределённость.

•Деликтная (внедоговорная) ответственность. Если киберинцидент причинил вред лицам, не состоящим в договоре, может применяться глава о возмещении вреда (деликт). Например, вследствие кибератаки на банк (охраняемый объект) утекли персональные данные клиентов, которые стали жертвами мошенничества. Клиенты банка не имеют договора с хакером (очевидно) или, возможно, с IT-провайдером банка, но они понесли вред. Они могут предъявить иск банку (как владельцу системы) на основании нарушения обязанностей по обеспечению безопасности их данных. Банк же, в свою очередь, если атака стала возможна из-за провайдера, может предъявить к нему регрессный иск или требование по договору. Однако для клиентов банку нужно доказать противоправность бездействия банка (например, несоблюдение требования закона о персональных данных по защите) и причинную связь с их ущербом. Такая деликтная ответственность за киберинциденты в узбекском праве не имеет специального регулирования, но аналогии можно провести с ответственностью за вред, причинённый источником повышенной опасности или оказанием услуг ненадлежащего качества. Пока что судебная практика Узбекистана по искам о компенсации вреда от утечки данных или кибератак практически отсутствует, что указывает на пробел и необходимость развития доктрины.

•Ответственность охранных организаций. Если охраняемый объект защищается по договору с частной охранной организацией, и произошёл киберинцидент (например, злоумышленник удалённо отключил сигнализацию и совершил кражу имущества), возникает вопрос: несёт ли охранная фирма ответственность за ущерб от кражи? Физически охранники могли действовать безупречно, но киберпробел привёл к инциденту. Формально, ответственность охранной организации наступает за неисполнение обязанностей по договору охраны – обычно это предотвращение несанкционированного проникновения. Если проникновение удалось из-за кибернарушения, можно утверждать, что охранная фирма не обеспечила комплекс-

ную защиту (не защитила канал связи, не проконтролировала ИТ-риски). Однако, если договор явно не оговаривал эти аспекты, привлечь охранную фирму к ответственности будет сложно – она может указать, что не обязана была противостоять хакерским методам, не предусмотренным договором. Этот пример показывает, насколько важно прописать кибербезопасность в договоре охраны. Пока же такие ситуации – серая зона ответственности.

•Ответственность государственных органов. В случаях, когда охраняемый объект – это, например, критическая инфраструктура, охраняемая государственным органом (МВД, Национальная гвардия по договору или закону), киберинцидент теоретически может повлечь ответственность государства, если будет доказано, что госорган не выполнил возложенных на него обязанностей по защите. Но, как правило, госорганы защищены иммунитетом от исков, и ущерб от кибератак на стратегические объекты покрывается либо государством (из бюджета), либо остаётся на потерпевшем (что нежелательно). В этом направлении законодательство только формируется; возможно, в будущем появятся нормы о компенсации государством вреда, причинённого в результате неспособности предотвратить кибератаку на критический объект, но сейчас такого прямого правила нет.

В целом, гражданско-правовая ответственность за киберинциденты в Узбекистане пока основывается на общих нормах договорного и деликтного права. Это приводит к неопределённости в оценке вины и распределении ущерба. Пострадавшие могут столкнуться с трудностями доказывания иска, а исполнители – с непредсказуемыми требованиями. Отсутствие прецедентов и разъяснений Верховного суда по таким делам усложняет задачу юристам при составлении договоров: они вынуждены максимально детализировать ответственность в контракте, чтобы не полагаться на неопределённые нормы.

Рекомендации по совершенствованию правового регулирования договорных отношений в области кибербезопасности

Для устранения выявленных пробелов и повышения эффективности гражданско-правового обеспечения кибербезопасности охраняемых объектов, представляется целесообразным реализовать ряд мер:

1.Разработка типовых договорных условий и стандартов. Государственным органам (например, Национальной гвардии, отвечающей за политику безопасности, или Минюсту) совместно с отраслевыми экспертами стоит разработать рекомендации или примерные образцы договоров на оказание услуг кибербезопасности. Такие стандарты могли бы включать: обязательные уровни сервиса (SLA) с минимально допустимыми показателями; требования к уведомлению о инцидентах (например, обязанность провайдера сообщить о любом серьёзном инциденте в течение 24 часов); обязанность иметь план реагирования и резервные меры; распределение ответственности и индемнити. Например, можно рекомендовать включать условие, что неуведомление о киберинциденте в срок само по себе является существенным нарушением договора. Это стимулирует оперативное информирование и позволяет заказчику разорвать контракт с недобросовестным исполнителем без долгих споров.

2.Изменения в законодательстве. Необходимо дополнить Закон "Об охранной деятельности" положениями о кибербезопасности охраняемых объектов. Например, ввести норму, что охранные организации при оказании услуг обязаны обеспечивать безопасность используемых ими технических и информационных систем, а в договорах охраны должны предусматриваться меры информационной безопасности охраняемого объекта. Это подтолкнёт включение соответствующих условий при заключении договоров и расширит ответственность охранных фирм за киберинциденты, связанные с их сферой деятельности. Кроме того, Закон "О кибербезопасности" мог бы быть дополнен главой о гражданско-правовом обеспечении: указать на необходимость договорного закрепления обязанностей при аутсорсинге киберзащиты, установить общие требования к таким договорам (по аналогии с требованиями к договорам в сфере связи или банковских услуг, которые иногда устанавливаются законодательством). Также следует рассмотреть внесение изменений в Гражданский кодекс – например, в главы о возмездном оказании услуг – указав, что услуги по обеспечению информационной безопасности имеют особый характер, и для них могут устанавливаться специальные правила ответственности. Это могут быть нормы о презумпции вины исполнителя при нарушении гарантированных уровней защиты, или об ограниченной возможности полностью освобождаться от ответственности за грубые нарушения кибербезопасности.

3.Уточнение режимов ответственности. Желательно на законодательном уровне или через постановления Пленума Верховного суда разъяснить применение норм ответственности к киберинцидентам. Например, разъяснить, что причинение имущественного вреда посредством кибератаки рассматривается судами аналогично причинению вреда имуществу физическим действием, и потерпевшие вправе требовать компенсации у ответственных субъектов (владельцев систем, обязанным их защищать). Отдельно можно рассмотреть возможность введения обязательства возмещения морального вреда гражданам при утечке их персональных данных вследствие киберинцидента – это стимулировало бы более серьёзное отношение компаний к защите данных. Закон о персональных данных Узбекистана такого права прямо не даёт, но его можно дополнить или опираться на общие нормы.

4.Внедрение требований к провайдерам услуг безопасности. Следует установить минимальные требования для компаний, предоставляющих услуги кибербезопасности охраняемых объектов. Например, обязательная сертификация таких провайдеров или нали-

чие лицензии на деятельность в сфере технической защиты информации. Если такие требования уже частично есть (через лицензирование телекоммуникационных услуг или охранной деятельности), их нужно адаптировать к киберсфере. Наличие сертификации/лицензии повысит ответственность: в случае систематических нарушений и инцидентов компания может лишиться права оказывать услуги. В договорах можно ссылаться на соответствие исполнителя требуемому стандарту (например, соответствие ГОСТ в сфере защиты информации или международному стандарту ISO 27001). Это также может быть критерием вины: несоответствие стандарту при оказании услуг будет считаться нарушением.

5.Поощрение киберстрахования и распределения рисков. Законодательно или через разъяснения стоит поощрять включение в договоры условий о страховании ответственности. Например, как условие договора крупного объекта с провайдером: последний обязан иметь действующий полис киберстрахования на сумму не менее определённой, и предоставить копию. Государство может стимулировать рынок киберстрахования, что облегчит бремя последствий инцидентов. Также можно рекомендовать ввести практику разделения рисков: часть риска остаётся на владельце объекта (например, форс-мажорные атаки государственного уровня), часть на провайдере (пропуск базовых мер безопасности).

6.Обучение и осведомленность сторон. Хотя это мера не законодательная, но методическая: необходимо повышать грамотность компаний и охранных организаций в вопросах кибербезопасности. Часто пробелы в договорах связаны банально с незнанием. Разработка руководств, проведение семинаров для юристов и менеджеров по киберрискам поможет при заключении договоров учесть все важные аспекты. Например, разъяснить, как правильно включать положения об ограничении ответственности, чтобы они были справедливы: не полностью снимать вину с провайдера, но и не отпугивать его неограниченными рисками Отдельно, обучение судей и адвокатов техническим аспектам кибербезопасности позволит качественно рассматривать споры и формировать практику.

Реализация этих рекомендаций позволит создать более сбалансированное и чёткое правовое поле для договорных отношений в сфере кибербезопасности охраняемых объектов. В результате каждая сторона будет понимать свои права и обязанности, а потерпевшие от кибератак – иметь гарантированные механизмы защиты и возмещения ущерба.

Заключение

Охраняемые объекты в современном мире – это не только стены и двери, но и коды, сети и данные. Гражданско-правовое обеспечение их кибербезопасности становится столь же важным, как и физическая охрана. Проведённый анализ показал, что в Узбекистане уже есть основы правового регулирования (законы о кибербезопасности, об охранной деятельности, о персональных данных), однако они обладают серьезными пробелами в части договорного регулирования и ответственности. Существующие договорные практики (контракты с провайдерами, SLA, соглашения о защите данных) работают, но не опираются на специальные нормы, а потому уязвимы к неоднозначному толкованию.

Для повышения киберустойчивости охраняемых объектов необходимо совершенствовать законодательство и практику: внедрять типовые договорные положения, уточнять зоны ответственности, стимулировать стандартизацию услуг кибербезопасности и использование страховых и иных механизмов распределения рисков. Четкое структурирование договорных отношений в этой сфере обеспечит баланс интересов: охраняемые объекты получат надежную защиту, исполнители – разумные пределы ответственности, а пострадавшие в случае инцидентов – уверенность в возможности возмещения.

В цифровую эпоху безопасность – это общий результат правовых, технических и организационных мер. Гражданско-правовые договоры играют роль “невидимого щита”, устанавливая правила игры для всех участников процесса обеспечения кибербезопасности. Усовершенствование этого щита на нормативном уровне – насущная задача, от решения которой зависит сохранность критически важных объектов и благополучие граждан в информационном обществе.

Источники:

1. Закон Республики Узбекистан "О кибербезопасности" № ЗРУ-764 от 15.04.2022 – принят первый комплексный акт, регулирующий отношения в сфере кибербезопасности. Устанавливает обязанности операторов критических объектов по обеспечению защиты информационных систем.

2. Dentons, обзор Закона "О кибербезопасности" (апрель 2022) – перечисляет ключевые требования к операторам критической инфраструктуры (непрерывность работы, резервное копирование, мониторинг, уведомление о инцидентах и др.).

3. Закон Республики Узбекистан "Об охранной деятельности" № ЗРУ-778 от 15.06.2022 – определяет охраняемый объект и основы физической охраны, однако не содержит норм о кибербезопасности (поиск по тексту на слово "кибер" не дал результатов).

4. Foley & Lardner LLP, рекомендации по включению кибербезопасности в договоры с внешними поставщиками (2024) – советуют предусматривать обязательное уведомление о утечках, планы реагирования, индемнити, ограничения ответственности и единые сроки уведомления.

5. Dunlap, Bennett & Ludwig, "Simple Steps to Limit Liability of Cybersecurity Service Providers" – подчёркивает необходимость подробных SLA, ограничительных оговорок об ответственности и наличия киберстрахования в договорах киберуслуг.