ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИИ ЦИФРОВЫХ УГРОЗ РЕСПУБЛИКИ УЗБЕКИСТАН

Азимжонов Дониербек Дилшод угли
Ташкентский государственный юридический университет
70420106- Право государственного управления
Тел: +998 97 2654400
thisisdoniyorlawyer@gmail.com
https://doi.org/10.5281/zenodo.15532235

ARTICLE INFO

Qabul qilindi: 20-May 2025 yil
Ma'qullandi: 25- May 2025 yil
Nashr qilindi: 28-May 2025 yil

KEYWORDS

персональные данные, правовая защита, цифровые угрозы, кибербезопасность, информационная безопасность, Узбекистан, GDPR.

ABSTRACT

В эпоху развития информационных технологий личные данные граждан подвергается к кибератаке, что требует основного внимания в совершенствование правовых инструментов защиты. Данная работа анализирует действующее законодательство Республики Узбекистан в сфере защиты персональных данных, проводя сравнительный анализ с международным опытом и стандартам и выявляя основные существующие пробелы в правовом регулировании. Особое внимание уделяется трем ключевым цифровым угрозам: несанкционированному доступу к персональным данным, их незаконной обработке и трансграничной передаче без надлежащих гарантий. Работа основана на анализе нормативно-правовых актов, международных соглашений и научных источников. Итоги работы подчеркивают необходимость в гармонизации национального законодательства с международными стандартами и предлагают конкретные меры по усилению защиты персональных данных Республики Узбекистан

Введение. В сегодняшнем современном цифровом обществе вопрос защиты персональных данных стала одним из приоритетных направлений государственной политики и правового регулирования. Активно развивающая цифровую экономику Республика Узбекистан, внедряя инновационные технологии во всей сферы жизни, сталкивается с новыми вызовами в области обеспечения безопасности граждан в информационной сфере.

Следует учесть, что цифровизация трансформирует глобальную экономику и общественные отношения, одновременно повышая риски цифровых угроз. В Узбекистане, где стратегия «Цифровой Узбекистан 2030» направлена на развитие электронного правительства, цифровизацию экономики и расширение доступа к интернету, защита персональных данных граждан становится основным элементом

национальной безопасности, а также обеспечения прав граждан (Указ Президента Республики Узбекистан, 2020).

Актуальность исследования обусловлена стремительным ростом цифровых угроз, которые все больше приобретают изощренные формы. В условиях развития сферы искусственного интеллекта, интернета и больших данных традиционные правовые механизмы защиты требуют существенного изменения и адаптации (Zuboff, 2019). К примеру, в 2023 году ГУП « Центр кибербезопасности» в ходе мониторинга сети интернета выявил базу учетных записей пользователей различных информационных ресурсов по всему миру, в том числе и в Республики Узбекистан, где были скомпрометированы 200 000 учетных записей и несут угрозы кибербезопасности в отношении информационной системы и ресурсов государственных органов (Kun.uz, 2023). В Узбекистане слабое правоприменение, ограниченное полномочие государственных органов и недостаточная киберграмотность населения препятствует эффективной защите данных, что требует комплексного анализа и реформ.

Методы. Методологическую основу исследования составляют общенаучные и специальные методы познания. А также использован системный подход при анализе национального законодательство, в частности, Закон Республики Узбекистан «О персональных данных» и поправки внесенные 2021 году, которые регулирующие защиту персональных данных, определяя правовые основы сбора, обработки и хранения данных (Закон Республики Узбекистан, 2019). Также проанализированы поправки и стратегия «Цифровой Узбекистан 2030», устанавливающая цели цифровизации. Метод позволил выявить юридические пробелы и оценить соответствие национального законодательства задачам цифровой трансформации.

Применены методы сравнительно-правового анализа для сопоставления национального законодательства с международными соглашениями и стандартами, в частности с Общим регламентом по защите данных Европейского союза (GDPR) и ведущих стран в области Киберправа и цифровизации государственной структуры. Анализ проводился по ключевым параметрам: права субъектов данных, обязанности операторов, механизмы правоприменения и санкции за нарушения.

Методология данного исследования обеспечивала комплексный подход, при этом сочетая нормативный анализ с эмпирическими данными, что позволило выявить проблемы и предложить научно обоснованные решения.

Результаты и обсуждение.

Система правового регулирования защиты персональных данных в Узекистан базируется на конституционных принципах, в частности **статья 31** Конституции Республики Узбекистан, где гарантируется право на неприкосновенности частной жизни, личную и семейную тайну, защиту своей чести и достоинства (Конституция Республики Узбекистан, 2023).

А также основные специальным актом является Закон Республики Узбекистан “О персональных данных” в котором регулируется отношение которые возникают процессе обработке и защите персональных данных. Однако анализ показывает существенные пробелы в правовом регулировании защиты персональных данных.

I. Статья 24 данного Закона предусматривает право субъекта не подвергаться решениям, которые основаны исключительно на автоматизированной обработке, но

не устанавливает четких требований к прозрачности алгоримов, их аудиту или объяснению логики принятия решений (Закон Республики Узбекистан, 2019). В отличии от GDPR статья 22, где требуется “право на объяснение” и конкретные ограничения на автоматизированные решения, влияющие на права граждан, то есть здесь Закон № ЗРУ-547 не деталищирует механизм защиты от дискриминации или ошибок алгоритмов (European Parliament and Council of the European Union, 2016).

По сравнению также в международных стандартах GDPR требует в прозрачности алгоритмов и права на оспаривание, именно в статьях 13-14 где устанавливается порядок предоставления персональных данных и их сбора от круга лиц (самого субъекта, третьего лица), а также их определенные право доступа к данным. К примеру, также можно взять зарубежный опыт Южной Корее, где законодательстве о персональных данных регулирует профилирование через обязательные аудиты (European Parliament and Council of the European Union, 2016).

В условиях цифровизации, включая системы OneID ил электронное правительство, отсутствие регулирования повышает риски необоснованных решений, например, в кредитовании или профилировании граждан. К примеру, утечка данных 2023 году наглядно показала уязвимости в автоматизированных системах, которые могли бы быть смягчены при наличии прозрачности алгоритмов и их уведомлений о нарушениях.

Для дальнейшего улучшения правопорядка в области обработки персональных данных, статья 24 Закона Республики Узбекистан требует ряд доработок с целью достижения к прозрачности алгоритмов, и внедрение обязательных аудитов внедряя искусственный интеллект как инструмент мониторинг, а также совершенствовать части прав субъектов на объяснение решений, как ведется в регулировании GDPR.

II. Также можно говорить об обработке биометрических и генетических данных, где в статье 26 Закона Республики Узбекистан “О персональных данных”, регулируется биометрические данные, требуя согласия субъекта, но не устанавливает конкретных тснадартов шифрования, хранения или уничтожения таких данных вне информационных систем.

Данная статья предусматривает поверхностный порядок использование и хранение биометрических и генетических данных в электронной форме вне информационных систем, а именно говорится об осуществления их только на материальных носителях информации исключающих несакционированный доступ к ним.То есть здесь нет определенных требований к сертификации материальных носителей или защиты от утечек данных. Например, требования к криптографической защите или соответствию международным стандартам (ISO/IEC 27001).

Также отсутсвуют конкретные меры защиты от утечек, такие как обязательное шифровние, многофакторная аутентификация или аудит безопасности носителей и нет требований к уничтожению биометрических данных после достижения целм обработки, что может увеличивать риски их неправомерного использования.

Если взять международный подход, то Общий регламент по защите данных (GDPR) предусматривает строгие меры для биометрических данных, включая риск-ориентированных подход. Статье 9 устанавливается, что биометрические данные являются специальной категорией и требует строгих мер защиты. Операторы обязаны

внедрять шифрование и проводить оценки воздействия на защиту данных для систем, обрабатывающих биометрические данные (European Parliament and Council of the European Union, 2016).

В качестве анализа можно взять также Сингапурский подход к обработке биометрических данных и в Законодательстве страны устанавливается обязательные технические меры как шифрование данных и уведомления о нарушениях (Personal Data Protection Commission Singapore, 2012).

Хотя известно, что биометрические данные (опечатки пальцев, сканирование лица) невозможно изменить, в отличие от паролей, что делает их утечку необратимой угрозой для субъектов. Но отсутствие шифрование и сертификации носителей увеличивает вероятность несанкционированного доступа, как в инциденте 2023 года.

А также слабая защита биометрических данных подрывает доверие граждан к системам электронного правительства и стратегии «Цифровой Узбекистан 2023», которая предусматривает расширение цифровых сервисов. И несоответствие международным стандартам ограничивает возможности Узбекистан в трансграничной передаче данных и сотрудничестве с глобальными технологическим компаниями. С целью предотвращения существующих угроз и принимая во внимание уязвимости в защите данных, применение дополнение в норме, может уменьшить риски и угрозы при обработке биометрических данных, установив требования к шифрованию, сертификации носителей и регулярным аудитам систем, обрабатывающих биометрические данные.

III. Если анализировать Закон Республики Узбекистан “О персональных данных”, можно заметить что в законе нету определенного требования об уведомления при случае нарушения в процессе обработки данных и нарушения безопасности данных. Данный Закон не устанавливает требования к операторам или собственникам баз персональных данных уведомлять субъектов данных или уполномоченный государственный орган о нарушение безопасности, таких как утечки данных, несанкционированный доступ или утрата данных.

Статья 31 № ЗРУ-547 определяет обязанности операторов, включая принятие мер по защите данных и уничтожение данных при достижении цели обработки, но не включает обязательство оперативного информирования о нарушениях. А также нет указаний на сроки и содержание таких уведомлений (Закон Республики Узбекистан, 2019).

Общий Регламент по защите персональных данных требует от операторов уведомлять надзорный орган о нарушении безопасности персональных данных в течение 72 часов после обнарушение, если нарушение может повлиять на права и свободы субъектов. Субъекты данных должны быть уведомлены без необоснованной задержки, если нарушение создает высокий риск. Уведомление должно содержать описание нарушения, возможные последствия и меры реагирования (European Parliament and Council of the European Union, 2016).

Если привести Сингапурский опыт, то в законодательство страны обязывает операторов уведомлять Комиссию по защите персональных данных о нарушениях как можно быстрее после оценки, если нарушение приведет к значительному ущербу или затронет более 500 лиц (Personal Data Protection Commission Singapore, 2012).

Отсутствие требования оперативных уведомлений Узбекистане препятствует своевременному реагированию на киберинциденты, увеличивая масштаб ущерба. И без обязательных уведомлений граждане не могут оперативно принять меры для защиты своих данных (например, сменить пароли или заморозить счета), что увеличивает риски мошенничества и финансовых потерь. Также отсутствие уведомлений ограничивает способность уполномоченного органа координировать реагирование и проводить расследования. Это также снижает подотчетность операторов, особенно в частном секторе (телеком, банки), где утечки могут замалчиваться.

Для устранения пробела, связанного с отсутствием обязательных уведомлений о нарушениях безопасности персональных данных в Законе № ЗРУ-547, предлагается комплекс мер, направленных на гармонизацию национального законодательства с международными стандартами (GDPR), а также на повышение эффективности реагирования на киберинциденты. Во-первых, целесообразно дополнить ЗРУ №-547 требованием, обязывающим операторов уведомлять уполномоченный государственный орган, о выявленных нарушениях безопасности в течение 72 часов с момента их обнаружения, что соответствует нормам GDPR.

IV. В Республике Узбекистан ответственность за нарушение требований Закона “О персональныйх данных” регламентируется положением статьи 33 которая отсылает к Кодексу “Об административном ответственности и Уголовному кодексу.

Статья 462 Кодекса Республики Узбекистан “об административном ответственности” устанавливает санкции за незаконный сбор, обработку или несоблюдение требований локалищации данных в размере 7 базовых расчетных величин для граждан и 50 БРВ для должностных лиц-“1-БРВ – 375 000 сум” (Кодекс Республики Узбекистан, 1994a).

А также предусмотрена Уголовная ответственность, которая применяется (ст. 141-2 УК) за повторное нарушение и наказывается штрафом в размере 100-150 БРВ или лишение определенных право до 3 лет (либо исправительные работы до 2 лет). При отягчающих обстоятельствах от 150 до 200 БРВ (Кодекс Республики Узбекистан, 1994b).

В совокупности в целом эти нормы образуют действующий в Республике Узбекистан механизм санкций за нарушения в области персональных данных.

Несмотря на нововведения, санкционный механизм Узбекистана имеет заметные пробелы. Во-первых, отсутствует пропорциональность наказания масштабу инцидента и размеру ущерба, то есть штрафы имеют фиксированную цену в абсолютных значениях. К примеру, без учета оборота компании, количества затронутых субъектов данных или характера нарушения. Так максимальный административный штраф единый для любых серьезных нарушений- будь то непреднамеренная техническая ошибка или умышленная массовая утечка.

Во-вторых, в законодательстве почти не прописаны критерии дифференциации санкций по степени виновности (умысел/небрежность), тяжести последствий, размера ущерба. А также отсутствуют гражданско-правовые механизмы компенсации пострадавшим, аналогично GDPR, и четкие требования к уведомлению о нарушениях. Все эти факторы снижают общий сдерживающий эффект существующих штрафов и

создают риск формального применения норм без учета реальной общественной опасности деяний.

В международной практике механизм санкций устроен иначе, и статья 83 GDPR предусматривает индивидуальный подход, где штрафы эффективны, пропорциональны и сдерживающи, и могут достичь 20 млн евро. При этом при расчете штрафов контролирующие органы учитывают природу, масштаб и продолжительность нарушения, количество пострадавших и другие фокторы (European Parliament and Council of the European Union, 2016). Это обеспечивает значительную вариативность санкций: от относительно умеренных для незначительных инцидентов до угрожающих существованию штрафов для крупных компаний .

Данный подход иллюстрирует, что эффективная система ответственности за нарушение персональных данных должна учитывать размер компании, характер нарушения и реальный ущерб. В сравнение с этим санкции Узбекистане выглядят значительно менее гибкими и масштабными. И практика применения санкций в Узбекистане пока ограничена. Известно, что ответственные органы включают нарушителей в реестр и блокируют их сайты. К примеру, 2021 году несколько иностранных сервисов (TikTok, ВКонтакте) подверглись ограничению доступа за несоблюдение локализации данных. Однако массовых реальных штрафов на крупные компании пока не фиксировалось. В отсутствие существенных экономических санкций крупные операторы могут воспринимать их как «плату за риск», что снижает общий сдерживающий эффект (Gazeta.uz, 2021).

Международный опыт свидетельствует, что лишь крупномасштабные штрафы, увязанные с доходами или масштабом деятельности, способны заставить большие организации серьёзно вкладываться в защиту данных.

Для совершенствования системы ответственности следует внедрить ряд изменений как установление принципа пропорциональности штрафов, а именно привязать максимальные размеры санкций к масштабу оператора (например, к годовой выручке или размеру базы данных) и тяжести нарушений, по образцу GDPR. А также следовательно можно ввести шкалу штрафов с учетом категории нарушителя и характера правонарушения. Данные меры позволят сделать наказания в области персональных данных более адекватным и сдерживающим, приближенным к международным стандартам. В конечном итоге это укрепит доверие граждан и повысить безопасность обработки персональных данных данных в стране.

Вывод.

Закон Республики Узбекистан «О персональных данных» создал правовую основу для защиты персональных данных, однако его ограничения существенно снижают эффективность регулирования в условиях роста цифровых угроз. Проведенное исследование выявило ряд юридических и институциональных пробелов, которые препятствуют обеспечению надежной защиты данных и реализации целей стратегии «Цифровой Узбекистан 2030». Отсутствие в статье 31 Закона требования к операторам уведомлять Государственный центр персонализации и субъектов данных о нарушениях безопасности, таких как утечки, является критическим пробелом. В отличие от GDPR данное упущение задерживает реагирование на инциденты, увеличивая их последствия. Утечка данных 2023 года, затронувшая более 200 000

учетных записей, продемонстрировала, как отсутствие оперативных уведомлений ограничивает возможности граждан защитить свои данные и подрывает прозрачность операторов. Введение обязательных уведомлений, включая четкие сроки, формат и каналы, позволит минимизировать ущерб и повысить подотчетность.

Закон также устанавливает ответственность за нарушения, но ограниченные штрафы не мотивируют операторов, особенно крупных, инвестировать в кибербезопасность. В сравнении с GDPR и PIPA, узбекские санкции не обладают сдерживающим эффектом. Это способствовало уязвимостям, приведшим к инциденту 2023 года, и снижению доверия к цифровым сервисам. Установление штрафов, пропорциональных доходу оператора, и введение административных мер, таких как приостановка деятельности, укрепят ответственность и стимулируют внедрение передовых мер безопасности.

Как сказали Закон также е содержит строгих стандартов сертификации, шифрования или аудита для биометрических данных, что контрастирует с GDPR. Учитывая рост использования биометрии в системах, таких как OneID, этот пробел увеличивает риски утечек биометрических данных. Введение обязательных стандартов (например, ISO/IEC 27001, AES-256) и регулярных аудитов позволит устранить уязвимости и обеспечить безопасность чувствительных данных.

Закон не обязывает операторов информировать граждан о мерах защиты после инцидентов, таких как смена паролей или мониторинг счетов, в отличие от PIPA. Развитие образовательных программ и введение обязанности операторов повышать осведомленность населения укрепят культуру кибербезопасности.

Сравнительный анализ с GDPR, PIPA и PDPA демонстрирует, что адаптация международных практик, включая оперативные уведомления, пропорциональные штрафы, строгие стандарты для биометрических данных, усиление надзора и повышение киберграмотности, позволит устранить выявленные пробелы. Реализация предложенных рекомендаций обеспечит соответствие национального законодательства вызовам цифровизации, укрепит доверие граждан к цифровым сервисам и поддержит достижение целей стратегии «Цифровой Узбекистан 2030», способствуя защите прав и свобод граждан в цифровой среде.

Список литературы:

1. Конституция Республики Узбекистан -Т. 01.05.2023 г.
2. Закон Республики Узбекистан «О персональных данных» № ЗРУ-547 от 02.07.2019 г. (с поправками 2023).
3. Кодекс Республики Узбекистан «об административной ответственности» от 01.04.1995 г.
4. Уголовный Кодекс Республики Узбекистан от 01.04.1995 г.
5.Указ Президента Республики Узбекистан «Об утверждении стратегии «Цифровой Узбекистан 2030» и мерах по ее реализации» от 5.10.2020 г. № УП-6079.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016.
5. Personal Information Protection Act (PIPA) of South Korea, Act No. 16930. 23.05.2020.
6. Personal Data Protection Act (PDPA) of Singapore, No. 26 of 2012
7. Voigt, P. The EU General Data Protection Regulation (GDPR): a practical guide / P. Voigt, A. Von dem Bussche. — Cham : Springer, 2017. — 317 c.

8. Zuboff, S. The age of surveillance capitalism: the fight for a human future at the new frontier of power / S. Zuboff. — New York : PublicAffairs, 2019. — 704 c.
9. Kun.uz. (2023, October 18). Персональные данные более 200 тысяч пользователей из Узбекистана утекли в сеть. https://m.kun.uz/news/2023/10/18
10. Gazeta.uz. (2021, October 14). Ограничение доступа к иностранным сервисам за несоблюдение локализации данных. https://www.gazeta.uz/ru/2021/10/14