

ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕСПУБЛИКЕ УЗБЕКИСТАН: АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА И ПРАКТИКИ ПРИМЕНЕНИЯ

<https://doi.org/10.5281/zenodo.20992617>

Набиев Иномжон Аюбхон ўғли

*Старший преподаватель кафедры цифровых
технологий и информационной безопасности,*

Аннотация

В данной статье рассматриваются актуальные проблемы регулирования персональных данных в Республике Узбекистан. Анализируется действующее законодательство, включая Закон Республики Узбекистан «О персональных данных», выявляются его недостатки и проблемы правоприменительной практики. Особое внимание уделяется вопросам локализации данных, недостаточного контроля, а также низкой осведомленности граждан. Делается вывод о необходимости совершенствования законодательства и усиления механизмов защиты персональных данных в условиях цифровизации.

Ключевые слова

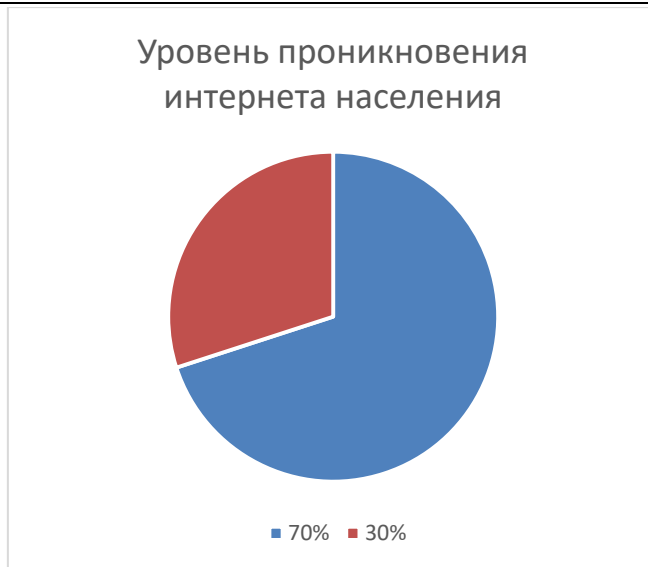
персональные данные, Республика Узбекистан, защита информации, цифровое право, локализация данных, информационная безопасность, конфиденциальность.

Abstract

This article examines the current problems of personal data regulation in the Republic of Uzbekistan. The legislation, including the Law "On Personal Data", is analyzed, and its shortcomings and enforcement issues are identified. Special attention is paid to data localization, weak control mechanisms, and low public awareness.

Keywords

personal data, data localization, data protection, information security, digital law, confidentiality.



В условиях глобализации и стремительного развития цифровых технологий наблюдается рост преступлений в сфере персональных данных, что ставит сложные задачи перед правоохранительными органами и органами государственной власти по выявлению, пресечению и предупреждению преступлений в сфере персональных данных. В Республике Узбекистан данная сфера регулируется Законом «О персональных данных» (№ ЗРУ-547 от 2 июля 2019 года). Несмотря на наличие нормативной базы, на практике возникает ряд существенных проблем, связанных с реализацией положений закона, его эффективностью и адаптацией к современным технологическим реалиям. Если посмотреть в статистику, то можно увидеть что из 38 миллионов граждан более 32 миллионов являются субъектами персональных данных. Уровень проникновения интернета превышает 70% населения. Это значит что основная информация о гражданах хранится в электронном виде в электронных базах Республики Узбекистан. И тут появляются несколько минусов закона

Ключевые проблемы регулирования персональных данных

Схематическое представление основных узких мест, выделенных в статье



Рисунок 1. Схематизация ключевых проблем регулирования персональных данных.

Почему правоприменение остаётся слабым

Логическая схема причин и последствий



Рисунок 2. Причины и последствия слабой реализации законодательства о персональных данных.

Проблема локализации данных это требование хранения данных исключительно на территории Республики Узбекистана, она увеличивает расходы бизнеса и ограничивает использование международных сервисов. Контроль осуществляет Государственный центр персонализации при Кабинете Министров Республики Узбекистан. И тут возникает проблема с глобальной IT-инфраструктурой. К примеру если сайт собирает данные пользователей из Узбекистана, это может считаться нарушением

локализации, даже если данные просто хранятся или используются только для аналитики. Проблема локализации персональных данных в Узбекистане заключается в том, что жёсткое требование хранения и обработки данных на территории страны вступает в противоречие с глобальной цифровой инфраструктурой, ограничивает использование международных сервисов, увеличивает издержки бизнеса и создаёт правовые риски при трансграничной передаче данных. К примеру 2021 году в стране заблокировали соцсеть TikTok, так как (компания ByteDance) не выполнила требования локализации персональных данных Республики Узбекистан. В эпоху развития технологии люди нашли способ обойти эту блокировку используя VPN, таким образом получая доступ к международным приложениям. Также локализация персональных данных может увеличить затраты бизнеса так как, строить “двойную инфраструктуру” (локальную + глобальную) это стоит больших вложений.

Под слабым контролем мы должны понимать что все данные о гражданах хранятся в серверах, расположенных на территории Республики Узбекистан, то есть механизм контроля и санкции применяются ограниченно. Уполномоченный орган – Государственный центр персонализации не обладает достаточной технической инфраструктурой для постоянного мониторинга, испытывает дефицит специалистов по кибербезопасности и аудиту. Слабая система правоприменения проверки носят эпизодический характер штрафы относительно невысокие → нет сильного сдерживающего эффекта сложно доказать факт хранения данных за рубежом. Например в 46²-статье об Административной ответственности штрафы физическим лицам – 7 БРВ (Базовая расчетная величина – 412 000 сумов), а юридическим лицам – 50 БРВ. Законом от 21.01.2026 г. № ЗРУ-1115 усиленные административные меры, дополнительно (особенно при использовании ИИ или технологий) штрафы 50–100 БРВ, возможен административный арест до 15 суток и конфискация оборудования. Если после административного наказания нарушение повторяется → применяется Уголовная ответственность по 141²-статье, штраф 150-200 БРВ, исправительные работы 2-3 года и лишение свободы до 3 лет. Но учитывая это, не законная хранения персональных данных приносит больше прибыли чем наказания, тем самым эти наказания в виде штрафа ничего не значат им.

Низкая осведомленность граждан о персональных данных – одна из ключевых проблем в сфере их защиты. Многие граждане не до конца понимают, какие сведения относятся к персональным данным, каким образом

они собираются, обрабатываются и передаются третьим лицам. На практике люди нередко без должной осторожности указывают паспортные данные, номера телефонов, адреса, сведения о банковских картах и иную чувствительную информацию на сайтах, в мобильных приложениях и социальных сетях. Недостаток правовой и цифровой грамотности приводит к тому, что граждане редко читают пользовательские соглашения, не знают о своих правах на доступ, исправление или удаление данных, а также не всегда способны распознать незаконный сбор информации. В результате низкая осведомленность повышает риск мошенничества, утечек данных и иных нарушений права на частную жизнь.

Итоги и предложения:

Анализ текущего состояния контроля локализации персональных данных в Узбекистане показывает, что при наличии формальной нормативной базы ключевой проблемой остается слабая практическая реализация требований. Это выражается в ограниченных возможностях надзора, недостаточной зрелости бизнеса и технологической зависимости от зарубежной инфраструктуры.

Регуляторные меры должны быть направлены на усиление правоприменения и создание реальных стимулов для соблюдения законодательства. В первую очередь, это введение санкций, соразмерных обороту компаний, что повысит их сдерживающий эффект. Также важно внедрить практику регулярных аудитов и обязательной отчетности по обработке и хранению персональных данных. Дополнительно следует разработать и внедрить систему сертификации дата-центров, обеспечивающую прозрачные требования к инфраструктуре хранения данных.

Технические меры предполагают развитие национальной цифровой инфраструктуры. Ключевым направлением является создание и масштабирование локальных дата-центров уровня Tier III и выше, способных конкурировать с зарубежными решениями по надежности и доступности. Параллельно необходимо стимулировать развитие локальных облачных провайдеров через экономические и регуляторные инструменты. Важным элементом также является создание технологических механизмов мониторинга трансграничной передачи данных, позволяющих выявлять нарушения в режиме, близком к реальному времени.

Организационные меры направлены на повышение уровня зрелости участников рынка. Это включает системное обучение бизнеса вопросам

compliance и подготовку специалистов по защите данных (DPO). Внедрение международных стандартов, таких как ISO/IEC 27001, должно стать нормой для компаний, работающих с персональными данными. Дополнительно необходимо повышать общий уровень цифровой грамотности, формируя у организаций и граждан понимание ценности и уязвимости персональных данных.

Предлагаемые направления совершенствования системы

Три блока мер, сформулированные в выводах статьи



Рисунок 3. Основные направления совершенствования системы защиты персональных данных.

В совокупности реализация данных мер позволит перейти от формального регулирования к эффективной системе контроля, обеспечивающей реальную защиту персональных данных и устойчивое развитие цифровой экономики страны.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Конституция Республики Узбекистан в новой редакции от 30.04.2023
2. Уголовно-процессуальный кодекс Республики Узбекистан 22.09.1994
3. Уголовный кодекс Республики Узбекистан 22.09.1994
4. Кодекс Республики Узбекистан об административной ответственности 22.09.1994
5. Закон Республики Узбекистан «О персональных данных» № ЗРУ-547 от 02.07.2019

6. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 №ЗРУ-764
7. Закон «Об информатизации» от 11.12.2003 № ЗРУ-560-II
8. Закон «О принципах и гарантиях свободы информации» от 12.12.2002 № ЗРУ-439-II
9. Закон "О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с регулированием отношений, возникающих при применении искусственного интеллекта" Республики Узбекистан от 21.01.2026 № ЗРУ-1115
10. Мирзаева, М. Б., & Абдазимов, С. З. (2022). Использование технологий искусственного интеллекта в сфере высшего образования.
11. Abdazimov, S., & Mustafa, D.. (2026). Zamonaviy axborot xavfsizligi tizimlarini loyihalash: ai va iot yondashuvlari ASOSIDA. Научный Фокус, 3(34), 313-321.
12. Abdazimov, S., & Mustafa, D.. (2026). Simmetrik kriptotizimlarda o'rniga qo'yish algoritmlarining qiyosiy tahlili va amaliy ahamiyati.
13. Научный Фокус, 3(34), 231-237.
14. Abdazimov, S., & Mustafa, D. (2026). Biometric authentication: modern methods of ensuring information security. Научный Фокус, 3(34), 222-230.
15. Abdazimov, Saidaminxo'dja., & (2022). Ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari. Central Asian Research Journal for Interdisciplinary Studies (CARJIS), 2(5), 109-115.