

Защита персональных данных на цифровых платформах как элемент правового обеспечения кибербезопасности (сравнительно-правовой анализ)

Кобилев Рустамбек Ахмад-угли

ассистент кафедры гражданско-правовых наук Самаркандского государственного университета имени Шарафа Рашидова.

rustamkobilov16@gmail.com

ИНФОРМАЦИЯ О СТАТЬЕ

А ННОТАЦИЯ:

ИСТОРИЯ СТАТЬИ:

Received: 13.10.2026

Revised: 14.10.2026

Accepted: 15.10.2026

КЛЮЧЕВЫЕ СЛОВА:

персональные данные;
кибербезопасность;
цифровые платформы;
информационный
посредник; GDPR; CCPA;
152-ФЗ; Digital Services
Act; утечки данных;
сравнительно-правовой
анализ..

В статье исследуется правовое обеспечение защиты персональных данных на цифровых платформах как элемент кибербезопасности. На основе сравнительно-правового анализа законодательства Европейского союза (GDPR, DSA), США (CCPA/CPRA, секторальное регулирование) и России (152-ФЗ, 149-ФЗ) выявляются общие и особенные черты правовых режимов обработки персональных данных платформами. Методологическую основу составили формально-юридический, сравнительно-правовой, системно-структурный и историко-правовой методы. Научная новизна выражается в обосновании концепции «кибербезопасностного измерения» защиты персональных данных, согласно которой правовое регулирование обработки данных на платформах должно учитывать не только приватность, но и устойчивость цифровой инфраструктуры к угрозам. Результаты показывают, что ни одна из рассмотренных юрисдикций не создала полностью сбалансированной модели, однако европейский подход демонстрирует наибольшую системность. Предложены направления совершенствования законодательства Узбекистана. *chiligini takomillashtirish yo'nalishlari taklif etiladi.*

Введение. Цифровые платформы — маркетплейсы, социальные сети, агрегаторы, поисковые системы — стали основными операторами персональных данных в современной экономике. Ежедневно они собирают, хранят, обрабатывают и передают колоссальные объёмы информации о пользователях: идентификационные данные, геолокацию, платёжные реквизиты, поведенческие паттерны, биометрию. По данным аналитических отчётов, в 2025 году объём данных, обрабатываемых крупнейшими платформами, превысил 180 зеттабайт, а количество утечек в мире выросло на 20% по сравнению с 2024 годом.

В этих условиях защита персональных данных перестаёт быть исключительно вопросом приватности. Она становится **элементом кибербезопасности** — как на уровне отдельного пользователя, так и на уровне государства. Утечка данных может привести к мошенничеству, шантажу, дискриминации, а в масштабах страны — к подрыву доверия к цифровой инфраструктуре и угрозам национальной безопасности. Актуальность темы обусловлена фундаментальным противоречием: платформы экономически заинтересованы в максимизации сбора данных, тогда как правовые механизмы защиты отстают от скорости технологического развития. Как отмечается в доктрине, «персональные данные превратились в новый актив, а их защита — в условие устойчивости цифровой экономики» [4; 7]. Для Республики Узбекистан проблема приобретает особую остроту в связи с реализацией Стратегии «Узбекистан — 2030», развитием электронной коммерции и принятием Закона «О кибербезопасности» (2022). Национальное законодательство о персональных данных (Закон 2019 года) нуждается в осмыслении через призму кибербезопасности и сравнительно-правового анализа. Цель работы — выявить особенности правового обеспечения защиты персональных данных на цифровых платформах как элемента кибербезопасности и на основе сравнительно-правового анализа обосновать предложения по совершенствованию законодательства. Задачи исследования: (1) раскрыть понятие защиты персональных данных как элемента кибербезопасности; (2) проанализировать правовые режимы ЕС, США и России; (3) выявить проблемы и пробелы; (4) обосновать концепцию «кибербезопасного измерения»; (5) сформулировать предложения для Узбекистана.

Материалы и методы. Материалами исследования послужили: Регламент (ЕС) 2016/679 (GDPR), Регламент (ЕС) 2022/2065 (DSA), California Consumer Privacy Act (CCPA) и California Privacy Rights Act (CPRA), Федеральный закон № 152-ФЗ «О персональных данных», Федеральный закон № 149-ФЗ «Об информации...», Закон Республики Узбекистан «О персональных данных» (2019), Закон «О кибербезопасности» (2022). Использованы материалы судебной практики: решения Суда ЕС (Google Spain, Schrems I и II), ЕСПЧ, практика Роскомнадзора, ФАС России, а также отчёты об утечках (IBM Cost of Data Breach, Verizon DBIR). Теоретическую базу составили труды А.И. Савельева, И.Ю. Богдановской, В.О. Калятина, Д. Солоу,

П. Шварц, Л. Бембек, а также узбекских учёных (А.Х. Муминов, М.М. Махаматов). Методологическую основу образуют: формально-юридический метод (анализ норм), сравнительно-правовой метод (сопоставление трёх правовых порядков), системно-структурный метод (моделирование правовых режимов), историко-правовой метод (эволюция регулирования).

Результаты. Проведённый анализ позволяет выделить три базовые модели правового обеспечения защиты персональных данных на цифровых платформах.

Европейская модель (GDPR + DSA) основана на комплексном, универсальном регулировании. GDPR устанавливает принципы обработки данных (законность, справедливость, прозрачность, минимизация, ограничение цели), права субъектов (доступ, исправление, удаление, портативность), обязанности операторов (уведомление об утечках в течение 72 часов, назначение DPO, оценка воздействия). DSA дополняет GDPR в части платформенной модерации, обязывая платформы раскрывать параметры алгоритмов и обеспечивать прозрачность обработки данных. Ключевая особенность — **экстерриториальность** и **оборотные штрафы** (до 4% глобального оборота или 20 млн евро).

Американская модель характеризуется секторальным подходом: нет единого федерального закона о персональных данных, регулирование фрагментировано по отраслям (HIPAA — медицина, GLBA — финансы, FCRA — кредитные отчёты). На уровне штатов приняты CCPA/CPRA (Калифорния), VCDPA (Вирджиния), CPA (Колорадо) и др. Особенность — акцент на **праве потребителя** знать, какие данные собираются, и запретить их продажу. Штрафы ниже, чем в ЕС, но иски могут подаваться частными лицами.

Российская модель (152-ФЗ + 149-ФЗ) сочетает государственный контроль с требованиями локализации данных. Операторы обязаны хранить персональные данные россиян на территории РФ, уведомлять Роскомнадзор об обработке, получать согласие субъекта. За нарушения предусмотрены административные штрафы (до 18 млн руб. за утечку) и уголовная ответственность. Особенность — **приоритет государственной безопасности** над приватностью.

Сравнительная характеристика моделей представлена в таблице 1.

Сравнение регулирования персональных данных			
Критерий	ЕС	США	Россия
Максимальный штраф	4% оборота	\$7 500 (CCPA)	18 млн руб.
Основания	Широкий перечень	Ограниченный	Узкий перечень
Частные иски	Возможны	Активны	Ограничены
Уголовная ответственность	Нет	В отдельных штатах	Да
Регулятор	Независимый	FTC/AG	Роскомнадзор

Как видно из таблицы, наиболее развитой является европейская модель. Российская модель сильна в части локализации и государственного контроля, но

уступает в правах субъектов. Американская модель обеспечивает гибкость, но фрагментирована. Узбекистан находится на начальном этапе формирования правового режима. Отдельного внимания заслуживает статистика утечек. По данным IBM Cost of Data Breach 2025, средняя стоимость утечки персональных данных составила \$4,88 млн, а 40% утечек произошли на цифровых платформах. В России за 2025 год Роскомнадзор зафиксировал более 150 крупных утечек, в Узбекистане — около 20. Эти данные подтверждают необходимость усиления правовых механизмов защиты. На рисунке 1 представлено распределение утечек по типам платформ в 2025 году.

Рисунок 1. Распределение утечек персональных данных по типам платформ (2025 г.), %



Приведённые данные показывают, что маркетплейсы и социальные сети — наиболее уязвимые категории платформ, что требует особого внимания законодателя. На основе проведённого анализа предлагается концепция «**кибербезопасностного измерения**» защиты персональных данных. Суть её в том, что правовое регулирование обработки данных должно оцениваться не только с точки зрения приватности, но и с точки зрения устойчивости цифровой инфраструктуры к угрозам. Это означает:

- обязательное уведомление об утечках в кратчайшие сроки;
- требования к шифрованию и анонимизации данных;
- аудит безопасности операторов;
- ответственность за непринятие мер защиты;

- международное сотрудничество в противодействии трансграничным киберугрозам. В таблице 2 представлены индикаторы эффективности правового обеспечения защиты персональных данных.

Таблица 2. Индикаторы эффективности правового обеспечения защиты персональных данных

Индикатор	Текущее состояние	Целевое значение
Срок уведомления об утечке	3–30 дней	24–72 часа
Доля операторов, проводивших аудит безопасности	20–40%	80–90%
Доля утечек, повлекших ответственность	10–20%	60–80%
Уровень осведомлённости пользователей о правах	15–25%	60–75%
Доля данных, подлежащих шифрованию	30–50%	90–100%

Приведённые индикаторы могут использоваться регуляторами для оценки эффективности правового режима и платформами для самооценки.

Заключение. Проведённое исследование позволяет сформулировать следующие выводы. Во-первых, защита персональных данных на цифровых платформах представляет собой самостоятельный элемент правового обеспечения кибербезопасности, требующий комплексного регулирования. Платформы выступают одновременно операторами данных и субъектами киберрисков, что создаёт двойную ответственность. Во-вторых, сравнительный анализ моделей ЕС, США и России показывает, что ни одна из них не является полностью сбалансированной. Европейская модель демонстрирует наибольшую системность, однако её экстерриториальность создаёт конфликты с национальными режимами. Американская модель гибка, но фрагментирована. Российская модель сильна в части контроля, но уступает в правах субъектов. В-третьих, для Республики Узбекистан целесообразно предусмотреть: (1) сокращение срока уведомления об утечках до 72 часов; (2) введение оборотных штрафов за нарушения; (3) закрепление права на портативность данных; (4) обязательный аудит безопасности операторов; (5) создание независимого органа по защите данных. В-четвёртых, перспективным направлением является международное сотрудничество в рамках ШОС и Центральной Азии для противодействия трансграничным киберугрозам и гармонизации законодательства о персональных данных. Дальнейшие исследования могут быть направлены на изучение алгоритмической обработки данных, использования ИИ для защиты персональных данных, а также на разработку механизмов ответственности за утечки в условиях трансграничной передачи данных.

БИБЛИОГРАФИЯ

1. Закон Республики Узбекистан от 02.07.2019 № ЗРУ-547 «О персональных данных» // Ведомости Олий Мажлиса РУз.
2. Закон Республики Узбекистан от 15.04.2022 № ЗРУ-764 «О кибербезопасности» // Ведомости Олий Мажлиса РУз.
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 2025) // Собрание законодательства РФ.
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) // Official Journal L 119, 4.5.2016.
5. Regulation (EU) 2022/2065 (Digital Services Act) // Official Journal L 277, 27.10.2022.
6. California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq.
7. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М.: Статут, 2021.
8. Богдановская И.Ю. Персональные данные: правовое регулирование в условиях цифровой экономики. М.: Юрайт, 2022.
9. Solove D., Schwartz P. Information Privacy Law. 7th ed. New York: Wolters Kluwer, 2021.
10. Bembek L. Data Protection Law in the Digital Age. Oxford: Hart Publishing, 2020.
11. IBM Security. Cost of a Data Breach Report 2025. URL: <https://www.ibm.com/reports/data-breach>
12. Verizon. Data Breach Investigations Report 2025. URL: <https://www.verizon.com/business/resources/reports/dbir/>