ПРАВОВЫЕ МЕХАНИЗМЫ ИМПОРТОЗАМЕЩЕНИЯ В СФЕРЕ ОБОРОТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ОТ ЛОКАЛИЗАЦИИ БАЗ ДАННЫХ К ТЕХНОЛОГИЧЕСКОМУ СУВЕРЕНИТЕТУ

А.С. Москаленко, *бакалавр*
Финансовый университет при Правительстве Российской Федерации (Россия, г. Москва)

DOI:10.24412/2500-1000-2026-6-2-320-325

Аннотация. *В статье исследуется эволюция правовых механизмов импортозамещения в сфере оборота персональных данных в Российской Федерации. Автор анализирует переход от концепции территориальной локализации баз данных к формированию комплексного технологического суверенитета. В работе исследуются актуальные нормативные правовые акты, регулирующие цифровую безопасность, а также выявляются коллизии в административном и уголовном законодательстве в части ответственности за утечки и нелегальный оборот личной информации. По итогам анализа предложены пути минимизации правовых рисков через введение института «доверенной среды обработки данных» и перспективную кодификацию информационного права.*

Ключевые слова: *персональные данные; импортозамещение; технологический суверенитет; локализация баз данных; информационная безопасность; правовое регулирование; утечка информации; СУБД.*

Трансформация подходов к обеспечению безопасности национального информационного пространства диктует необходимость переосмысления базовых институтов ИТ-сферы. Фокус государственного регулирования сместился с пассивного контроля над зарубежными вендорами в сторону форсированного создания замкнутых технологических циклов. Процесс импортозамещения, начавшийся как реакция на санкционные ограничения, перерос в стратегию достижения абсолютного цифрового суверенитета. В правовой плоскости ключевой точкой напряжения стал оборот персональных сведений, требующий сопряжения интересов бизнеса, прав граждан и императивов национальной безопасности.

Инфраструктурная изоляция российского ИТ-рынка обнажила уязвимость зарубежных программных комплексов и СУБД, применявшихся для обработки сведений о гражданах. Долгое время отечественное законодательство опиралось на концепцию локализации баз данных, закрепленную в Федеральном законе № 242-ФЗ. Первоначальный этап требовал лишь физического нахождения серверов на территории страны. Сегодняшние реалии доказывают недостаточность пространственного размещения материальных носителей без контроля над программным обеспечением и микроэлектроникой. Смена парадигмы диктует необходимость конструирования жестких юридических ограничений, стимулирующих переход на суверенный софт.

Генезис институтов локализации данных в российском праве

Нормативная база, регулирующая требования к сбору и хранению личной информации, изначально формировалась в логике интеграции в глобальное цифровое пространство. Статья 18 Федерального закона «О персональных данных» № 152-ФЗ зафиксировала обязанность операторов обеспечивать запись, систематизацию, накопление, хранение, уточнение и извлечение личных сведений граждан Российской Федерации с использованием баз данных, расположенных исключительно на ее территории. На практике бизнес столкнулся с технологической неготовностью к резкому разрыву связей с трансграничными облачными платформами. Правоприменитель же пошел по пути администрирования формального присутствия серверов, упуская из виду архитектурную зависимость систем управления базами данных (СУБД) от иностранных правообладателей.

Существующие юридические коллизии порождают неопределенность статуса операторов. Исследователи справедливо подчеркивают дефицит четких формулировок, разграничивающих зоны ответственности участников

информационного обмена [4]. Специфика сетевой архитектуры Интернет позволяет обходить материальные границы государств, создавая дублирующие контуры обработки информации за пределами национальной юрисдикции [7]. Юридическая фикция локализации зачастую маскирует реальное использование зарубежного проприетарного софта, контролируемого удаленно через системы обновлений и технической поддержки. Подобная практика нивелирует защитную функцию законодательства.

Полагаем, ценность территориального размещения серверов без автономии программного стека стремится к нулю в условиях санкционного давления. Государство осознает риски одномоментного отключения критических ИТ-сервисов. Законодатель начал усложнять требования, связывая локализацию с реестрами отечественного программного обеспечения и радиоэлектронной продукции. Происходит переход от плоскостной географической привязки данных к созданию многоуровневого правового щита, исключающего иностранное программное присутствие в критических узлах инфраструктуры.

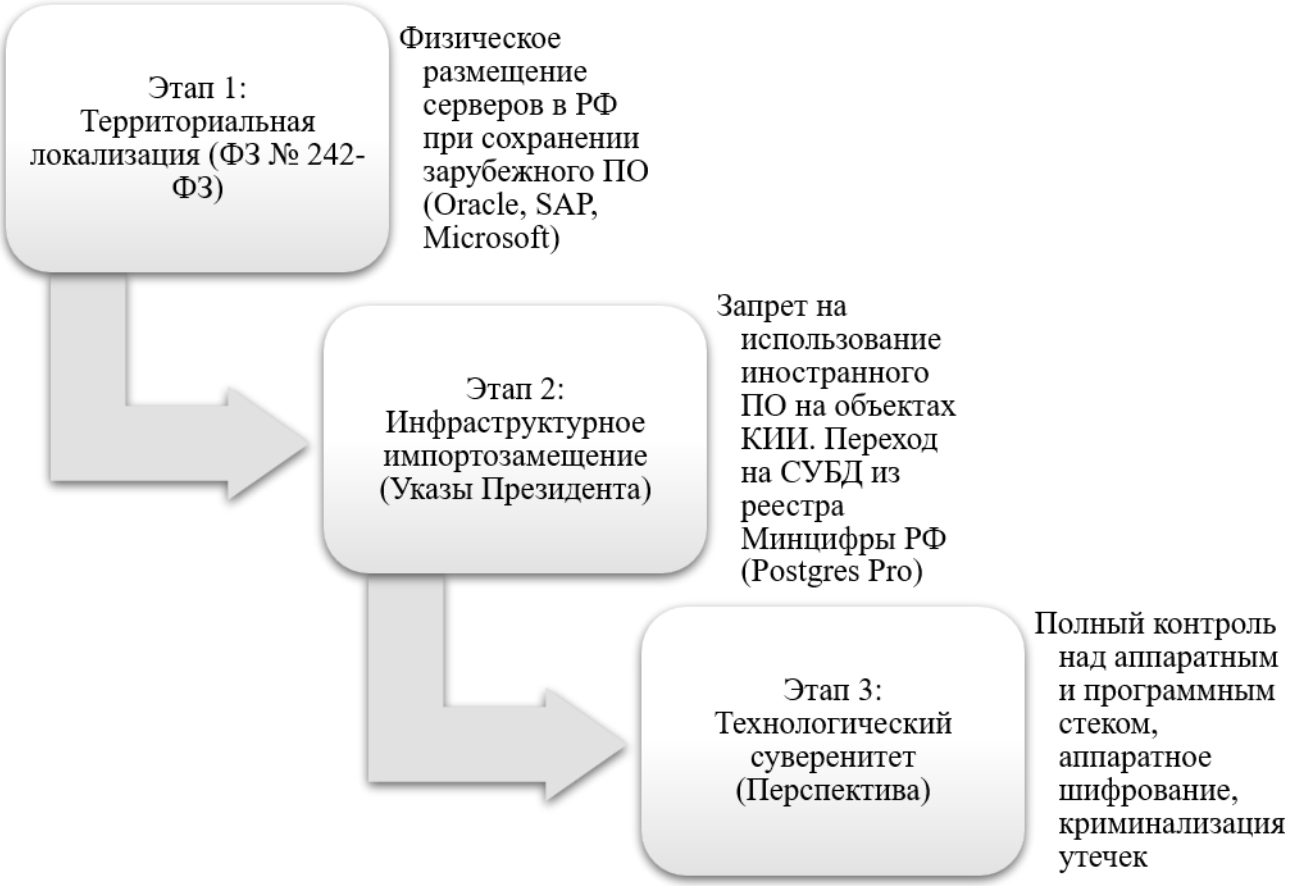

Рис. 1. Эволюция правовых механизмов оборота данных

Административно-правовые и уголовно-правовые барьеры

Инструментарий принуждения к замещению иностранных технологий включает механизмы контроля со стороны Роскомнадзора, ФСТЭК и ФСБ. Административные регламенты стали жестче, требования к трансграничной передаче информации пересмотрены в сторону резкого ограничения субъектного состава получателей. Исследования структуры государственного управления указывают на внутренние противоречия ведомственных нормативных актов, снижающие общую эффективность защитных мер [5]. Отсутствие сквозных стандартов аудита безопасности СУБД позволяет недобросовестным операторам использовать серые схемы обработки сведений с привлечением облачных мощностей дружественных юрисдикций, не гарантирующих суверенный контроль.

Параллельно обостряется проблема нелегального оборота сведений, выходящая за рамки административных деликтов. Масштабные утечки личной информации из баз данных крупных ритейлеров и финансовых организаций приобрели характер угрозы национальной безопасности. В экспертном сообществе активно обсуждаются инициативы по реформированию материального уголовного права в части криминализации действий лиц, осуществляющих незаконный сбор, хранение и распространение массивов личной информации [1]. Действующая редакция Уголовного кодекса РФ (включая статьи 137 и 272) не охватывает специфику современных компьютерных преступлений, связанных с компиляцией «пробитых» баз данных из открытых и закрытых источников.

Очевидна потребность в дифференциации составов преступлений, совершаемых в киберпространстве. Охрана легального оборота информации требует синхронизации норм уголовного права с динамично меняющимся ИТ-законодательством [2]. Рост числа киберугроз делает необходимым создание специальных криминалистических методик. Зарубежный опыт, в частности сравнительный анализ подходов Российской Федерации и США, демонстрирует преобладание в отечественной практике штрафных санкций над механизмами реального возмещения вреда и изоляции правонарушителей [9]. Данное обстоятельство снижает превентивный потенциал государственного принуждения.

Авторы статьи убеждены, что без жесткой уголовной ответственности за создание черных рынков данных невозможно стимулировать бизнес вкладывать средства в дорогую суверенную инфраструктуру. Пока покупка украденной базы обходится дешевле внедрения сертифицированных отечественных средств защиты, импортозамещение рискует остаться декларативным процессом. Законодательное закрепление оборотных штрафов и введение реальных сроков лишения свободы за незаконный экспорт баз данных должны стать катализаторами перехода корпоративного сектора на российские платформы.

Переход к технологическому суверенитету: правовое измерение

Понятие технологического суверенитета в сфере информации шире классического импортозамещения. Последнее предполагает простую замену зарубежного аналога отечественным, что часто сводится к переклеиванию ярлыков на китайском оборудовании или форканью опенсорсных программных продуктов без изменения их архитектурного ядра. Истинный суверенитет требует создания собственной экосистемы, включающей правовые стандарты разработки софта, суверенную криптографию и независимые каналы связи. Персональные данные здесь выступают в роли стратегического ресурса, топливного элемента для обучения национальных нейросетевых моделей, чья безопасность напрямую зависит от используемой программной среды.

Правовое обеспечение перехода к новому технологическому укладу базируется на указах Президента РФ, регламентирующих запрет на использование иностранного программного обеспечения на объектах критической информационной инфраструктуры (КИИ). Нормотворчество в данной сфере сталкивается со скрытым сопротивлением крупных операторов связи и банковских конгломератов. Причина проста: перенос колоссальных массивов данных с СУБД Oracle или SAP на условный Postgres Pro требует миллиардных инвестиций и сопряжен с рисками временной потери управляемости бизнес-процессами.

Юридическая наука рассматривает личную информацию не только как объект охраны, но и как ключевой элемент персональной защиты человека в цифровой среде [3]. Размывание границ частной жизни вследствие тотальной платформизации требует адекватных правовых ответов. Законодателю приходится балансировать между фискально-контрольными интересами государства и конституционными правами граждан на неприкосновенность личной сферы. Безопасность не может достигаться за счет ликвидации права на конфиденциальность.

Эффективное регулирование трансграничного перемещения информации видится невозможным без учета международно-правового контекста. Глобальные вызовы требуют создания новых двусторонних и многосторонних соглашений, регулирующих оборот информации, особенно в рамках макрорегиональных объединений вроде БРИКС и ЕАЭС [6]. Национальное законодательство должно быть готово к интеграции с дружественными правовыми

системами при сохранении жесткого контроля над суверенным ядром ИТ-инфраструктуры. Формирование закрытых контуров обмена данными становится условием выживания государств в условиях геополитического разлома.

Мы полагаем, ключевым элементом правового механизма суверенизации должно стать нормативное закрепление понятия «доверенная среда обработки данных». Юридический статус такой среды обязан включать требования не только к происхождению софта, но и к отсутствию скрытых функциональных возможностей (бэкдоров), проверяемому на уровне исходного кода. Право оператора на трансграничную передачу информации должно быть жестко увязано с использованием исключительно сертифицированных отечественных средств криптографической защиты информации (СКЗИ). Такой подход позволит трансформировать пассивную оборонительную позицию локализации в проактивную модель технологического доминирования на внутреннем рынке.

Риски и пробелы правового регулирования на современном этапе

Анализ нормативных актов показывает наличие пробелов в регулировании процессов деанонимизации больших данных (Big Data). Операторы часто обходят требования закона № 152-ФЗ, подвергая массивы сведений процедуре поверхностного обезличивания, позволяющей восстановить личность конкретного гражданина с помощью простейших алгоритмов сопоставления. Юридическая неопределенность статуса подобных массивов информации создает риски их неконтролируемого экспорта за рубеж под видом маркетинговой или аналитической информации. Проблема усугубляется отсутствием легального определения правового режима искусственного интеллекта, выступающего главным потребителем данных.

Уголовно-правовая доктрина также демонстрирует отставание от технологического прогресса. Квалификация деяний, связанных с незаконным оборотом криптографически защищенных сведений, вызывает затруднения у органов предварительного расследования и судов [8]. Существующие пробелы в понятийном аппарате не позволяют эффективно разграничивать преступления против компьютерной информации и посягательства на неприкосновенность частной жизни. Ситуация осложняется транснациональным характером киберпреступности, когда организаторы утечек находятся вне зоны досягаемости российского правосудия.

Таблица 1. Сравнительная характеристика моделей локализации баз данных и технологического суверенитета

Критерий сравнения	Локализация баз данных (Прошлый этап)	Технологический суверенитет (Текущий этап)
Основное правовое требование	Физическое нахождение серверов на территории РФ	Использование ПО из реестра Минцифры, отечественного оборудования
Объект контроля	Географическая точка размещения дата-центра	Весь стек технологий: от микросхем до прикладного софта
Характер защиты	Формально-юридический (наличие договора аренды мощностей)	Архитектурно-технический (отсутствие зарубежных уязвимостей)
Трансграничный оборот	Разрешен при соблюдении формальных процедур уведомления	Жестко ограничен, требует фильтрации через суверенные шлюзы

По нашему мнению, устранение указанных дефектов законодательства требует не точечных правок, а коренной кодификации информационного права. Создание Цифрового кодекса РФ могло бы решить проблему внутренней противоречивости институтов защиты информации. Нормы, регулирующие оборот персональных сведений, интеллектуальную собственность на алгоритмы СУБД и стандарты информационной безопасности, необходимо свести в единую систему. Только системная интеграция материально-правовых и процессуальных норм позволит завершить переход от примитивного замещения импортного софта к созданию автономного цифрового пространства.

Заключение

Правовые механизмы обеспечения импортозамещения в сфере оборота личных сведений проделали значительный путь от примитивного требования территориального размещения серверов до комплексных систем

обеспечения технологической независимости. Эволюция законодательства отражает изменение характера угроз, сместившихся из плоскости защиты прав отдельных субъектов в сферу противодействия межгосударственному кибернетическому противоборству. Локализация баз данных выполнила свою историческую задачу, подготовив инфраструктурную базу для последующих реформ.

Дальнейшее развитие правового регулирования должно быть направлено на ликвидацию серых зон в сфере оборота больших данных и ужесточение ответственности за нарушение правил их обработки. Создание суверенного технологического стека требует не только административных запретов, но и формирования стимулирующих правовых режимов для отечественных разработчиков СУБД и средств защиты информации. Обеспечение баланса между интересами национальной безопасности и правами граждан на неприкосновенность частной жизни остается главным вызовом для законодателя на пути к достижению цифрового суверенитета.

Библиографический список

1. Панина Н.Н. Совершенствование правовых механизмов привлечения к уголовной ответственности за незаконный оборот персональных данных / Н.Н. Панина // Уголовно-правовое обеспечение правоохранительной деятельности: взгляд молодежи : Материалы научно-практической конференции, проведенной в рамках I Съезда Молодежной секции Международного союза криминалистов, Москва, 27 сентября 2024 года. – Москва: Московская академия следственного комитета, 2024. – С. 211-215. – EDN SZYJHM.

2. Кур И.Н. Целесообразность совершенствования уголовно-правовых механизмов охраны оборота персональных данных и компьютерной информации / И.Н. Кур // Уголовная политика России на современном этапе: состояние, тенденции, перспективы : Сборник научных трудов по материалам международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Г.А. Аванесова. В 2-х частях, Москва, 27 сентября 2024 года. – Москва: Академия управления МВД России, 2024. – С. 151-156. – EDN RVIEFO.

3. Синдянкин Н.Н. Персональные данные как элементы персональной защиты в правовой сфере современной действительности / Н.Н. Синдянкин // Теория и практика кооперации в современном обществе: материалы Международной научно-практической конференции, Саранск, 23-24 апреля 2025 года. Часть 1. – Саранск: РИЦ МГПУ, 2025. – С. 243-246. – EDN QCXKCT.

4. Яковлева-Чернышева А.Ю. проблемы правовой определенности положений законодательства в сфере правовой защиты персональных данных / А.Ю. Яковлева-Чернышева, Р.Н. Данелян, В.А. Яковлев-Чернышев // Вестник Российской правовой академии. – 2023. – № 3. – С. 113-127. – DOI 10.33874/2072-9936-2023-0-3-113-127. – EDN DXBUHE.

5. Адажук А.С. Проблемы нормативного правового регулирования административно-правового механизма защиты персональных данных в Российской Федерации / А.С. Адажук // Гуманитарный научный журнал. – 2025. – № 7. – С. 83-90. – DOI 10.24412/2078-9661-2025-7-1-2. – EDN VRRBBX.

6. Александров А.Д. Правовое регулирование трансграничного оборота данных и защита персональной информации / А.Д. Александров, Г.В. Вахонин // Modern Science. – 2024. – № 12-1. – С. 12-15. – EDN TVFWSV.

7. Ерболатов Е.Е. Особенности правового регулирования оборота персональных данных в сети Интернет / Е.Е. Ерболатов // Вестник Торайгыров университета. Юридическая серия. – 2023. – № 2. – С. 43-58. – DOI 10.48081/EMGR5259. – EDN TEGHJF.

8. Анисимова Е.С. Проблемные вопросы уголовно-правового регулирования незаконного оборота персональных данных / Е.С. Анисимова, К.А. Степанова // Модель Федерального Собрания РФ: Материалы V научно-практической конференции студентов и молодых учёных, Екатеринбург, 20-21 марта 2025 года. – Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2025. – С. 146-157. – EDN DNNFCC.

9. Магарченков Н.А. Реализация ответственности за неправомерный оборот персональных данных в России и США: сравнительно-правовой анализ / Н.А. Магарченков // Многонациональная Россия: вчера, сегодня, завтра. – Смоленск: Смоленский государственный университет, 2025. – С. 599-606. – EDN RYPNZG.

LEGAL MECHANISMS OF IMPORT SUBSTITUTION IN THE SPHERE OF PERSONAL DATA TURNOVER: FROM DATABASE LOCALIZATION TO TECHNOLOGICAL SOVEREIGNTY

A.S. Moskalenko, *Bachelor*
Financial University under the Government of the Russian Federation
(Russia, Moscow)

Abstract. *The article examines the evolution of legal mechanisms for import substitution in the field of personal data turnover in the Russian Federation. The author analyzes the transition from the concept of geographical data localization to the formation of comprehensive technological sovereignty. The paper explores current regulatory legal acts governing digital security and identifies conflicts in administrative and criminal legislation regarding liability for data leaks and illicit turnover of personal information. Based on the results of the analysis, the author proposes ways to minimize legal risks through the introduction of the «trusted data processing environment» institution and the prospective codification of information law.*

Keywords: *personal data; import substitution; technological sovereignty; data localization; information security; legal regulation; data leak; DBMS.*