Белов М.Э. Персональные данные: локализация «первичной записи» и архитектура комплаенса // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с.118–132

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056:342.721:004.6:004.03.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЛОКАЛИЗАЦИЯ «ПЕРВИЧНОЙ ЗАПИСИ» И АРХИТЕКТУРА КОМПЛАЕНСА

Белов М.Э.
ФГБОУ ВО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ», Донецк, Россия (283001, Донецкая народная республика, г. Донецк, Университетская ул., д. 24), e-mail: mark_1998boss@mail.ru

В статье анализируется требование локализации «первичной записи» персональных данных в условиях современных распределённых IT-архитектур. Показано, что отсутствие легального определения первичной записи и расхождение между юридическим и техническим пониманием фиксации данных формируют системные риски несоблюдения требований локализации даже при формальном размещении баз данных на территории Российской Федерации. На основе анализа нормативного регулирования, правоприменительной практики и типовых архитектур цифровых платформ предложена техническая модель архитектуры комплаенса, обеспечивающая контролируемую точку первичной записи, управление потоками персональных данных и проверяемость соответствия требованиям законодательства. Модель ориентирована на практическое применение в IT-аудите, regtech-инструментах и проектировании информационных систем.

Ключевые слова: LegalTech, локализация, первичная запись, ч.5 ст.18 152-ФЗ, трансграничная передача, ст.12 152-ФЗ, архитектура комплаенса, ИСПДн, 1119, ФСТЭК-21, риск-ориентированный подход.

PERSONAL DATA: LOCALIZATION OF THE "PRIMARY RECORD" AND COMPLIANCE ARCHITECTURE

Belov M.E.
DONETSK NATIONAL UNIVERSITY, Donetsk, Russia (283001,Donetsk People's Republic Donetsk, Universitetskaya St., 24), e-mail: mark_1998boss@mail.ru

This article analyzes the requirement to localize the "primary record" of personal data in the context of modern distributed IT architectures. It is shown that the lack of a legal definition of the primary record and the discrepancy between the legal and technical understanding of data recording create systemic risks of non-compliance with localization requirements, even when databases are formally located within the Russian Federation. Based on an analysis of regulatory frameworks, law enforcement practices, and typical digital platform architectures, a technical model of compliance architecture is proposed that ensures a controlled primary record point, management of personal data flows, and verifiability of compliance with legal requirements. The model is designed for practical application in IT audits, regulatory technology tools, and information system design.

Keywords: LegalTech, localization, primary recording, Part 5 of Article 18 of Federal Law No. 152, cross-border transfer, Article 12 of Federal Law No. 152, compliance architecture, ISPDN, 1119, FSTEC-21, risk-oriented approach.

Введение

Актуализация требований к локализации персональных данных в 2025 году обозначила качественный сдвиг в правовом регулировании обработки данных, сместив фокус с формального контроля места хранения к регулированию архитектуры процессов их сбора и первичной фиксации. Усиление акцента на локализацию «первичной записи» выявило

системное противоречие между юридическим пониманием момента начала обработки персональных данных и технической логикой функционирования современных распределённых IT-систем. В научной литературе отмечается, что действующее правовое регулирование персональных данных исторически ориентировано преимущественно на централизованные модели обработки информации и в ограниченной степени учитывает специфику распределённых архитектур и микросервисных систем [5],[8]. В результате формируется разрыв между нормативным толкованием «записи» персональных данных и фактическими процессами их фиксации и передачи в IT-системах, что порождает риски формального соблюдения требований локализации при их фактическом нарушении. Настоящая статья направлена на анализ данного противоречия и обоснование перехода от декларативного комплаенса к архитектурно ориентированному подходу. В работе предлагается авторская модель архитектуры комплаенса, обеспечивающая проверяемую локализацию первичной записи персональных данных и синхронизацию нормативных требований с реальной технической организацией процессов обработки данных.

1. Теоретико-нормативные основания локализации персональных данных

1.1. Эволюция требований к локализации персональных данных

Требования к локализации персональных данных сформировались как часть более общего процесса развития правового регулирования в сфере защиты информации и обеспечения цифрового суверенитета. На первоначальном этапе регулирование было ориентировано преимущественно на обеспечение конфиденциальности и безопасности данных как объекта правовой охраны, без жёсткой привязки к месту их физического размещения [5, с. 42,].

С развитием цифровых платформ и трансграничных информационных потоков акцент регулирования сместился в сторону территориального контроля обработки персональных данных. В российском праве данный подход был закреплён во введении требования локализации персональных данных граждан Российской Федерации, установленного в с. 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», согласно которому запись, систематизация, накопление и хранение персональных данных должны осуществляться с использованием баз данных, расположенных на территории Российской Федерации [1, с. 18].

Изначально указанное требование в правоприменительной практике трактовалось преимущественно как требование к месту хранения и систематизации данных. Однако усложнение архитектуры информационных систем и переход к распределённым моделям обработки выявили ограниченность такого подхода, поскольку территориальный контроль исключительно над базами данных не охватывает этапы сбора и первоначальной фиксации персональных данных [6, с. 117].

Указанное противоречие было нормативно устранено в результате изменений, внесённых **Федеральным законом от 30.11.2024 № 420-ФЗ**, вступивших в силу с **1 января 2025 года**, которыми в с. 18 152-ФЗ был прямо усилен акцент на локализацию **первичной записи персональных данных** при их сборе [2, с. 18]. Тем самым законодатель зафиксировал, что соблюдение требования локализации должно обеспечиваться уже на этапе первоначальной фиксации данных, а не только на стадии их последующего хранения. Данное

изменение знаменует переход от формального территориального контроля к содержательному регулированию архитектуры процессов обработки персональных данных.

1.2. Понятие «первичной записи» персональных данных

В юридическом смысле под первичной записью персональных данных понимается момент первоначальной фиксации персональных данных оператором, с которого начинается их обработка и возникают предусмотренные законодательством обязанности по обеспечению локализации и защиты данных [1, с. 3]. В правоприменительной практике именно данный момент рассматривается как юридически значимый для определения применимой юрисдикции и объёма обязанностей оператора.

В техническом смысле первичная запись представляет собой первое персистентное сохранение персональных данных в устойчивом компоненте информационной системы — базе данных, журнале событий, event-store или очереди сообщений, — допускающем восстановление, воспроизведение и использование данных в бизнес- или аналитических процессах [9, с. 45]. Такое сохранение принципиально отличается от временного нахождения данных в оперативной памяти или транзитной передаче.

В юридической доктрине первичная запись традиционно связывается с возникновением правовых последствий и началом обработки персональных данных [7, с. 64]. Однако данный подход носит абстрактный характер и не учитывает архитектурную специфику современных распределённых информационных систем, в которых персональные данные могут фиксироваться поэтапно и в различных компонентах инфраструктуры [8, с. 89]. Это затрудняет однозначное определение момента и места первичной записи и формирует зону правовой неопределённости.

В целях устранения указанного разрыва в рамках настоящего исследования предлагается авторское комплексное определение:
первичная запись персональных данных — это первый юридически значимый и технически персистентный акт фиксации персональных данных в контролируемом компоненте информационной системы оператора, с которого данные становятся доступными для последующей обработки, воспроизведения или анализа и с которого должны обеспечиваться **требования локализации и защиты персональных данных**.

Данное определение позволяет синхронизировать нормативное и техническое понимание первичной записи и использовать его как основу для архитектурного проектирования и оценки соответствия требованиям законодательства.

1.3. Аспекты противоречия между нормативным и техническим пониманием момента «первичной записи»

В технической архитектуре информационных систем фиксация персональных данных носит принципиально иной характер и представляет собой распределённый процесс, включающий приём запросов, временное хранение данных в памяти, буферизацию, кэширование, логирование и асинхронную обработку [9, с. 134]. В результате момент, который в праве рассматривается как единичный акт записи, в IT-системах распадается на последовательность технических операций, не всегда очевидных для оператора и юридической функции.

В распределённых архитектурах персональные данные могут быть зафиксированы в логах, аналитических модулях или инфраструктуре внешних сервисов до их поступления в основное хранилище, которое оператор формально считает локализованным. Это приводит к ситуации, при которой фактическая первичная фиксация персональных данных осуществляется за пределами контролируемой юрисдикции при формальном соблюдении требований законодательства [10, с. 98].

Таким образом, выявляемое противоречие указывает на ограниченность трактовки локализации персональных данных исключительно как требования к месту хранения информации. В условиях современных IT-архитектур локализация приобретает характер архитектурного свойства системы, зависящего от проектных решений, определяющих маршруты данных и точки их фиксации. Указанное обстоятельство обосновывает необходимость перехода от формального нормативного подхода к архитектурно ориентированному пониманию локализации «первичной записи», что и определяет дальнейшую логику исследования.

2. Архитектура современных IT-систем обработки персональных данных

2.1. Типовая цепочка обработки персональных данных

Современные IT-системы обработки персональных данных, как правило, строятся на принципах распределённой архитектуры и включают несколько функциональных уровней, каждый из которых участвует в процессе фиксации и передачи данных. Типовая цепочка обработки начинается с пользовательского интерфейса — веб- или мобильного приложения, через которое субъект персональных данных вводит информацию. На данном этапе данные формируются в виде структурированных запросов и могут временно сохраняться в памяти устройства или браузера [11, с. 56].

Далее данные передаются через API-шлюзы, выполняющие функции маршрутизации, аутентификации и предварительной обработки запросов. API-шлюзы нередко осуществляют логирование входящих запросов, что уже на этом этапе создает дополнительную точку фиксации персональных данных [12, с. 143]. Серверы приложений обеспечивают бизнес-логику обработки данных, их валидацию и последующую передачу в хранилища.

Отдельное место в архитектуре занимают аналитические и логирующие сервисы, предназначенные для мониторинга, сбора метрик и анализа пользовательского поведения. Такие сервисы могут обрабатывать идентификаторы пользователей, IP-адреса и иные сведения, относящиеся к персональным данным, зачастую в автоматическом режиме [13, с. 211]. Дополнительно в цепочку обработки включаются внешние сервисы и SDK, предоставляемые третьими лицами, что существенно усложняет контроль над потоками данных и местом их первичной фиксации.

2.2. Точки возникновения и фиксации персональных данных

В рамках описанной архитектуры персональные данные могут возникать и фиксироваться на различных уровнях системы. Уже на уровне пользовательского интерфейса и API-шлюзов формируются потенциальные точки первичной записи, что требует их рассмотрения не только как элементов передачи данных, но и как архитектурных компонентов, критичных для соблюдения требований локализации. На клиентской стороне фиксация данных происходит в момент их ввода пользователем и формирования сетевого

запроса. Несмотря на то, что такие данные часто рассматриваются как «необработанные», они уже могут быть сохранены в логах браузера, мобильного приложения или инструментов отладки.

На серверной стороне фиксация персональных данных осуществляется при приёме запросов, их обработке и записи в базы данных. Однако помимо основного хранилища данные могут сохраняться во временных буферах, очередях сообщений и логах серверных компонентов, что создает дополнительные точки записи [15, с. 98].

Особую категорию составляют сторонние сервисы аналитики и мониторинга, которые могут получать персональные данные параллельно с основной обработкой. Такие сервисы нередко функционируют в иной юрисдикции и используют собственную инфраструктуру хранения данных [16, с. 162]. В результате «первичная запись» персональных данных может происходить до того, как данные поступят в локализованную базу оператора, что противоречит его представлениям о контролируемой точке фиксации.

2.3. Проблема распределённой фиксации данных

Ключевой архитектурной особенностью современных IT-систем является распределённый характер фиксации персональных данных. Использование механизмов буферизации и кэширования приводит к временному сохранению данных в различных компонентах системы, не всегда находящихся под прямым контролем оператора [17, с. 121]. Асинхронная передача данных, характерная для микросервисных архитектур, дополнительно размывает границы между моментом сбора и моментом окончательной записи данных.

Значительную роль в распределённой фиксации играют журналы событий и системные логи, которые предназначены для диагностики и обеспечения отказоустойчивости. В таких журналах могут содержаться персональные данные или их производные, что фактически образует самостоятельные точки первичной записи [18, с. 87]. При этом данные журналы зачастую не рассматриваются оператором как элементы системы обработки персональных данных.

Таким образом, архитектура современных IT-систем создает ситуацию, при которой фиксация персональных данных осуществляется множественно и распределённо, а момент «первичной записи» может предшествовать осознанной обработке данных оператором. Это, в свою очередь, формирует существенные риски несоблюдения требований локализации, которые рассмотрены в следующем разделе.

3. Риски несоблюдения локализации «первичной записи» персональных данных

3.1. Архитектурные риски обработки персональных данных

Распределённая архитектура современных IT-систем формирует совокупность архитектурных рисков, связанных с неконтролируемой фиксацией персональных данных. Одним из ключевых рисков является наличие множественных точек записи данных, не учитываемых оператором при проектировании системы. Такие точки могут возникать в API-шлюзах, промежуточных сервисах, очередях сообщений и логирующих компонентах, которые изначально не рассматриваются как элементы обработки персональных данных [12, с. 146].

Использование облачных инфраструктур и внешних SDK дополнительно усиливает данные риски. Персональные данные могут временно или постоянно фиксироваться в инфраструктуре третьих лиц, что затрудняет определение юрисдикции первичной записи и

контроль за соблюдением требований локализации [8, с. 91]. В условиях микросервисной архитектуры оператор нередко утрачивает целостное представление о потоках данных, поскольку отдельные компоненты системы разрабатываются и обслуживаются независимо друг от друга [17, с. 129].

Следствием указанных архитектурных особенностей становится ситуация, при которой фактическая первичная фиксация персональных данных происходит вне локализованного контура, несмотря на размещение основной базы данных на территории требуемой юрисдикции. Это создает структурный риск несоответствия требованиям законодательства, не связанный с умышленными действиями оператора.

3.2. Правовые и комплаенс-риски

В соответствии с законодательством о персональных данных ответственность за соблюдение требований обработки возлагается на оператора независимо от используемых технических решений и привлечения третьих лиц [1, с. 18].

В правоприменительной практике это означает, что формальное размещение баз данных на территории соответствующей юрисдикции не освобождает оператора от ответственности в случае выявления фактов первичной фиксации данных за её пределами. При этом доказательство архитектурной добросовестности оператора осложняется отсутствием документированной модели потоков данных и явных точек первичной записи [6, с. 121].

Дополнительным комплаенс-риском является разрыв между юридической и технической интерпретацией обработки персональных данных. Юридическая функция, как правило, опирается на договоры, политики и реестры процессов, тогда как реальные точки фиксации данных определяются архитектурными решениями, принятыми на уровне разработки и эксплуатации системы [10, с. 102]. В результате комплаенс приобретает декларативный характер и не отражает фактическое состояние системы.

3.3. Практика регуляторного и судебного толкования первичной записи персональных данных

Практика Роскомнадзора и судебных органов Российской Федерации свидетельствует о расширительном толковании требования локализации персональных данных, при котором ключевое значение придаётся не только месту хранения баз данных, но и архитектуре процессов их сбора и первичной фиксации. В рамках контрольно-надзорной деятельности регулятор исходит из того, что первичная запись персональных данных может осуществляться на ранних этапах обработки, включая момент их передачи в сторонние сервисы и программные компоненты.

Показательным является дело LinkedIn Corporation (дело № А40-18827/2016). В решении Московского городского суда от 10.11.2016 указано, что сбор и обработка персональных данных пользователей осуществлялись с использованием серверной инфраструктуры, расположенной за пределами Российской Федерации, что образует нарушение требований с. 18 Федерального закона № 152-ФЗ. Суд фактически связал нарушение не только с хранением данных, но и с архитектурой их первичного сбора, признав юридически значимым момент первоначальной фиксации персональных данных пользователей.

Аналогичный подход отражён в практике Таганского районного суда г. Москвы по делам о привлечении к ответственности Twitter Inc. и Meta Platforms Inc. (Facebook) (дела № 05-

1927/2021, № 05-1196/2022). В указанных делах суд исходил из того, что персональные данные российских пользователей фиксируются и обрабатываются в зарубежной инфраструктуре на этапе их сбора, что свидетельствует о несоблюдении требований локализации независимо от последующего хранения отдельных массивов данных.

Практика Роскомнадзора в отношении российских операторов также подтверждает архитектурный характер толкования первичной записи. В ходе проверок и разъяснений 2021–2023 гг. регулятор указывал на недопустимость использования сервисов веб-аналитики Google Analytics без обеспечения локализации первичной фиксации пользовательских данных, включая IP-адреса и идентификаторы, передаваемые в инфраструктуру Google LLC в момент взаимодействия пользователя с сайтом.

В научной литературе подобный подход объясняется объективным усложнением архитектуры обработки данных и направлен на предотвращение формального соблюдения требований локализации при фактическом выведении процессов первичной фиксации за пределы национальной юрисдикции.

4. Архитектура комплаенса как ответ на регуляторные требования

4.1. Понятие архитектуры комплаенса

Таким образом, усложнение цифровых систем и распределённый характер обработки персональных данных выявили ограниченность традиционного понимания комплаенса как совокупности формальных документов, регламентов и договорных обязательств. Такой подход не отражает фактические процессы фиксации и передачи данных в современных IT-архитектурах и не позволяет обеспечить проверяемое соблюдение требований законодательства. В этой связи в научной и прикладной литературе используется понятие архитектуры комплаенса, под которой понимается совокупность архитектурных решений, обеспечивающих встроенное соответствие информационной системы нормативным требованиям [9, с. 37].

Архитектура комплаенса предполагает рассмотрение правовых требований не как внешних ограничений, а как проектных параметров системы, учитываемых при формировании её структуры и логики функционирования. Такой подход соответствует концепции *compliance by design*, согласно которой соблюдение правовых норм обеспечивается архитектурой системы, а не исключительно последующим контролем или аудитом [16, с. 174]. В сфере персональных данных это означает, что требования локализации и контроля первичной записи должны быть реализованы на уровне архитектуры обработки данных.

Таким образом, архитектура комплаенса может быть определена как способ формализации правовых требований в виде устойчивых архитектурных свойств информационной системы. Вне такой формализации комплаенс носит декларативный характер и не оказывает влияния на фактическую организацию процессов обработки персональных данных [6, с. 127].

4.2. Компоненты архитектуры комплаенса и их соответствие НПА

Под компонентами архитектуры комплаенса в рамках настоящего исследования понимаются **структурно и функционально выделенные элементы IT-архитектуры**, через которые реализуются требования законодательства о персональных данных и подзаконного регулирования. В отличие от формального подхода, при котором требования 152-ФЗ, ПП РФ

№ 1119 и приказа ФСТЭК № 21 фиксируются в документации, архитектурный подход предполагает их прямую реализацию в конкретных технических контурах обработки данных.

Регуляторную основу данных компонентов составляют положения Федерального закона № 152-ФЗ «О персональных данных», а также подзаконные акты, конкретизирующие его требования: Постановление Правительства РФ от 01.11.2012 № 1119, устанавливающее уровни защищённости ИСПДн, и приказ ФСТЭК России от 18.02.2013 № 21, определяющий обязательные меры защиты информации. С 2025 года данные требования дополняются усиленным акцентом на локализацию **первичной записи персональных данных**, что требует явного архитектурного закрепления соответствующих этапов обработки.

Ключевым компонентом архитектуры комплаенса является **Primary Data Ingress (PDI)** — архитектурно выделенная точка приёма персональных данных. В нормативном смысле данный компонент реализует требования с. 18 152-ФЗ и ПП РФ № 1119 в части контроля этапа сбора данных. В практической реализации PDI, как правило, представляет собой API Gateway или backend-for-frontend, совмещённый с механизмами фильтрации и контроля трафика. Его основная функция заключается в предотвращении несанкционированной первичной фиксации персональных данных в сторонних сервисах и обеспечении того, чтобы момент первичной записи происходил исключительно в контролируемом локализованном контуре.

Primary Storage Layer (PSL) отвечает за выполнение требований законодательства, связанных с локализацией, хранением и защитой персональных данных. Данный компонент реализуется в виде локализованного устойчивого хранилища (база данных или event-store), размещённого на территории Российской Федерации и защищённого в соответствии с приказом ФСТЭК № 21. С практической точки зрения PSL является технически и юридически значимой точкой начала обработки персональных данных, поскольку именно в нём осуществляется их первичное персистентное сохранение, подлежащее контролю и аудиту.

Функции **Data Classification Middleware (DCM)** соотносятся с требованиями ПП РФ № 1119 о необходимости классификации ИСПДн и определения уровня их защищённости. В практической архитектуре DCM реализуется в виде middleware или policy-engine, автоматически присваивающего данным и операциям обработки соответствующий статус. Значение данного компонента заключается в формализации регуляторных требований и снижении риска ошибочной или избыточной передачи персональных данных за пределы допустимого контура.

Outbound Control Layer (OCL) реализует положения приказа ФСТЭК № 21, касающиеся контроля сетевых взаимодействий и предотвращения утечек информации. На практике OCL внедряется на уровне сетевой инфраструктуры или service mesh и обеспечивает контроль всех исходящих потоков данных. Его роль заключается в техническом обеспечении запрета передачи персональных данных за пределы локализованного контура до момента их допустимой трансформации, что имеет ключевое значение для соблюдения требований локализации первичной записи.

Таким образом, архитектурное выделение и согласованная реализация компонентов PDI, PSL, DCM и OCL позволяет трансформировать требования законодательства и подзаконных актов в устойчивые технические свойства информационной системы. Учет данных компонентов формирует основу для построения авторской модели архитектуры комплаенса, ориентированной на проверяемое и доказуемое соблюдение обновлённых требований о локализации первичной записи персональных данных, вступивших в силу с 2025 года.

5. Техническая модель обеспечения локализации первичной записи персональных данных

5.1. Формализация архитектурной модели первичной записи

В целях практической реализации требований локализации «первичной записи» персональных данных предлагается техническая архитектурная модель, основанная на **жёстком разграничении этапов фиксации данных и их последующей обработки**.

В рамках настоящего исследования под архитектурной моделью первичной записи персональных данных понимается **формализованная последовательность технических и логических операций обработки данных**, выстроенная таким образом, что момент и место первичной записи персональных данных однозначно фиксируются в пределах территории Российской Федерации, а последующие операции обработки допускаются только после завершения данной записи и в нормативно допустимой конфигурации потоков данных.

В рамках данной модели первичная запись трактуется не абстрактно, а как конкретная операция записи данных в устойчивое хранилище или журнал событий, обладающее следующими признаками:

1. возможность восстановления данных после сбоя;
2. возможность их последующего воспроизведения;
3. использование в бизнес- или аналитических процессах.

Таким образом, первичная запись приравнивается к первому персистентному сохранению персональных данных в архитектуре системы [9, с. 45].

5.2. Совокупная модель архитектуры первичной записи персональных данных

Предлагаемая модель архитектуры первичной записи персональных данных основана на жёстко заданной и технически детерминированной последовательности этапов обработки данных, при которой каждый последующий этап логически и архитектурно невозможен без завершения предыдущего. Модель исключает параллельные, опережающие либо неявные операции записи и передачи персональных данных за пределы первичного контура до момента их нормативно корректной фиксации, что обеспечивает однозначное определение момента и места первичной записи.

Этап 1. Инициация сбора персональных данных (pre-collection stage). На первом этапе субъект персональных данных инициирует взаимодействие с информационной системой (заполнение формы, обращение к сервису, использование функционала приложения). На данном этапе допускается обработка исключительно неидентифицирующих технических данных, необходимых для установления соединения и функционирования протоколов передачи информации (например, параметры сетевого соединения, служебные заголовки запросов).
Любая фиксация данных, позволяющих прямо или косвенно идентифицировать субъекта персональных данных, на данном этапе архитектурно исключается и не рассматривается как первичная запись.

Этап 2. Первичная запись идентифицируемых данных (PDI/PSL stage). На втором этапе осуществляется первая и единственная первичная запись персональных данных, позволяющих идентифицировать субъекта. Данный этап реализуется исключительно через компонент Primary Data Ingress (PDI) с последующей записью данных в Primary Storage Layer (PSL), развернутые в пределах инфраструктуры, физически и логически расположенной

на территории Российской Федерации. Юридически именно этот момент квалифицируется как «сбор персональных данных» в смысле части 5 статьи 18 Федерального закона № 152-ФЗ. Технически он выражается в операции персистентного сохранения персональных данных в устойчивом хранилище или журнале событий без предварительной передачи, репликации или обработки данных во внешних сервисах, аналитических SDK или вспомогательных контурах.

Этап 3. Формирование псевдонимизированных идентификаторов (post-record stage).

Только после завершения первичной записи персональных данных система формирует устойчивые технические идентификаторы (токены, session ID, client ID), используемые для последующей обработки данных и взаимодействия между компонентами системы. Указанные идентификаторы логически связаны с первичной записью, однако не содержат персональных данных в явном виде и не позволяют идентифицировать субъекта без обращения к первичному контуру хранения.

Этап 4. Классификация данных и управление потоками (DCM stage). На данном этапе осуществляется контролируемая маршрутизация и дальнейшая обработка данных с использованием Data Classification Middleware (DCM). Архитектура модели обеспечивает, что:

- идентифицируемые персональные данные не покидают первичный контур без наличия правового основания;
- псевдонимизированные и агрегированные данные могут использоваться для аналитических и сервисных целей;
- любые попытки отклонения от установленной последовательности обработки блокируются на уровне маршрутизации и политик передачи данных.

Тем самым реализуется нормативно обусловленный поток данных (data flow), при котором направление, содержание и допустимость передачи данных определяются не функциональной целесообразностью, а требованиями законодательства о персональных данных.

Этап 5. Фиксация и подтверждение корректности обработки (OCL stage). Заключительный этап модели направлен на фиксацию и подтверждение соблюдения установленной архитектурной последовательности обработки персональных данных. В рамках данного этапа формируются журналы первичной записи, метаданные маршрутизации, логи сетевых и прикладных операций, а также реестр интеграций и технических зависимостей, контролируемых через Outbound Control Layer (OCL). Наличие данного слоя позволяет воспроизвести полную цепочку обработки персональных данных и подтвердить, что первичная запись была осуществлена до любых операций последующей обработки, логирования, аналитики или передачи данных во внешние сервисы, что устраняет архитектурную неопределённость момента фиксации персональных данных [12, с. 158].

5.3. Критерии аудита и проверки реализации модели

Для практического применения предложенная архитектурная модель допускает формализованную проверку соответствия, ориентированную на воспроизводимый IT-аудит и доказуемость соблюдения требований локализации первичной записи. В отличие от

документального комплаенса, который фиксирует намерения оператора, техническая верификация модели должна подтверждать фактическое поведение системы: где именно происходит первичная запись, какие компоненты получают доступ к данным и в какой последовательности выполняются операции обработки.

Критерий 1. Наличие единственной точки первичной записи. Верификация включает подтверждение того, что в архитектуре существует ровно одна контролируемая точка, в которой идентифицируемые персональные данные впервые сохраняются персистентно (PSL), а любые альтернативные маршруты (прямой доступ клиента к сервисам, запись через обходные эндпоинты, «теневые» очереди или журналы) исключены. На практике данный критерий проверяется через анализ конфигураций API, сетевых политик и фактических маршрутов запросов.

Критерий 2. Отсутствие логов и метрик, содержащих персональные данные, до PSL.

Проверка предусматривает анализ логирования на всех этапах до первичной записи: на уровне клиентских SDK, API Gateway, middleware, балансировщиков и систем мониторинга. Требование означает, что до PSL допускается фиксация только технических параметров, не позволяющих идентифицировать субъекта, а персональные данные должны быть исключены из логов и метрик либо замещены безопасными маркерами. Это снижает риск неявной первичной записи в логирующем контуре.

Критерий 3. Документированная и актуальная схема data flow. Модель предполагает наличие архитектурно утверждённой схемы потоков данных, отражающей последовательность этапов обработки: от пользовательского интерфейса до первичного хранилища и далее до контуров аналитики и внешних интеграций. Для аудита значима не только наличие схемы, но и её подтверждаемость наблюдаемыми техническими артефактами (маршрутизация, политики egress, конфигурации сервисов).

Критерий 4. Технические ограничения на SDK и внешние API. Доказуемость модели обеспечивается не декларативными запретами, а техническими ограничениями: контролем исходящего трафика, запретом прямых вызовов внешних сервисов до PSL, а также регламентом допустимых данных, которые могут покидать локализованный контур (только псевдонимизированные или агрегированные). В рамках аудита проверяется наличие механизма принудительного исполнения этих ограничений.

Критерий 5. Трассируемость данных от интерфейса до хранилища. Критически важным элементом является возможность воспроизвести цепочку обработки персональных данных и показать, что первичная запись предшествует любой дальнейшей обработке или передаче. Трассируемость достигается за счёт корреляционных идентификаторов, журналов событий, метаданных маршрутизации и контроля доступа, что позволяет проводить расследования инцидентов и подтверждать соответствие модели [10, с. 109].

Перечисленные критерии позволяют использовать предложенную модель как практическую основу для **IT-аудита**, **регуляторных проверок** и **regtech-инструментов автоматизированного контроля**, в которых соответствие проверяется по наблюдаемым техническим признакам, а не по декларативным документам.

5.4. Границы применимости модели

Предложенная архитектурная модель локализации первичной записи персональных данных ориентирована на практическое применение в информационных системах, архитектура которых допускает выделение контролируемого первичного контура обработки данных. Наибольшую эффективность модель демонстрирует в системах с централизованным backend-контуром, в рамках которого возможно архитектурно зафиксировать единственную точку первичной записи и обеспечить нормативно обусловленную последовательность обработки данных. В таких системах компоненты PDI, PSL, DCM и OCL могут быть чётко разграничены и поддаются техническому аудиту и трассировке, что позволяет реализовать проверяемый комплаенс.

Дополнительным условием применимости модели является наличие контролируемого набора внешних интеграций. Архитектура предполагает, что все взаимодействия с аналитическими, мониторинговыми и сторонними сервисами осуществляются через формализованные каналы передачи данных, допускающие техническое ограничение состава и статуса передаваемой информации. При таком подходе становится возможным исключить неявную первичную фиксацию персональных данных во внешних компонентах и обеспечить соответствие требованиям локализации первичной записи.

В высоко-распределённых системах, использующих событийно-ориентированные архитектуры, большое количество автономных микросервисов и внешних SDK, реализация модели сталкивается с дополнительными ограничениями. В таких условиях контроль последовательности обработки и предотвращение несанкционированной фиксации данных требуют внедрения дополнительных уровней orchestration, централизованного управления событиями и расширенных механизмов event-control. Это приводит к росту архитектурной сложности, увеличению эксплуатационных затрат и повышенным требованиям к управлению конфигурациями и политиками безопасности [8, с. 104].

Таким образом, предложенная модель не претендует на универсальное применение во всех типах информационных систем, однако она задаёт архитектурный ориентир и набор проектных принципов, которые могут быть адаптированы и масштабированы в зависимости от уровня распределённости системы и требований к контролю обработки персональных данных.

Заключение

Проведённое исследование показало, что усиление требования локализации «первичной записи» персональных данных с 2025 года обусловлено не столько расширением объёма обязанностей операторов, сколько необходимостью устранения системного разрыва между юридическим и техническим пониманием процессов обработки данных. Анализ нормативных источников и правоприменительной практики подтвердил, что формальное размещение баз данных на территории Российской Федерации не гарантирует соблюдение требований законодательства в условиях распределённых IT-архитектур, в которых фиксация персональных данных может происходить множественно и асинхронно.

В рамках работы предложено авторское комплексное определение первичной записи персональных данных как первого юридически значимого и технически персистентного акта фиксации данных в контролируемом компоненте информационной системы оператора. Данное определение позволяет синхронизировать абстрактные правовые категории с

реальными архитектурными решениями и устранить неопределённость момента начала обработки персональных данных.

Существенным результатом исследования является анализ компонентов архитектуры комплаенса (PDI, PSL, DCM, OCL) и их соотнесение с требованиями Федерального закона № 152-ФЗ и подзаконного регулирования. Показано, что нормативные требования могут быть реализованы не декларативно, а в виде устойчивых архитектурных свойств информационной системы, поддающихся технической верификации и аудиту.

На основе проведённого анализа разработана авторская модель архитектуры локализации первичной записи персональных данных, основанная на жёстко детерминированной последовательности этапов обработки и исключающая неявную фиксацию данных за пределами локализованного контура. Предложенная модель формирует практическую основу для проверяемого комплаенса, IT-аудита и regtech-инструментов и может быть использована операторами персональных данных при проектировании и модернизации информационных систем в условиях обновлённого регулирования.

Список литературы

1. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ
2. «О персональных данных» (ред. действующая на 2025 г.) // Собрание законодательства РФ. — 2006. — № 31 (ч. 1). — С. 3451.
3. Российская Федерация. Законы. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 ноября 2024 г. № 420-ФЗ // Официальный интернет-портал правовой информации.
4. Российская Федерация. Правительство. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : Постановление Правительства РФ от 01 ноября 2012 г. № 1119
5. Федеральная служба по техническому и экспортному контролю. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (ред. от 14.05.2020) : зарегистрировано в Минюсте России 14.05.2013 № 28375 // КонсультантПлюс.
6. Бачило И. Л. Право информационных технологий : учебник для вузов. — 2-е изд., перераб. и доп. — М. : Юрайт, 2020. — 419 с.
7. Кучерена А. Г. Информационная безопасность и защита персональных данных. — М. : Норма, 2019. — 304 с.
8. Лопатин В. Н. Правовые основы защиты персональных данных в цифровой среде // Журнал российского права. — 2021. — № 3. — С. 58–71.
9. Kuner C. Transborder Data Flows and Data Privacy Law. — Oxford : Oxford University Press, 2017. — 392 p.
10. Bass L., Clements P., Kazman R. Software Architecture in Practice. — 3rd ed. — Boston : Addison-Wesley, 2012. — 624 p.
11. Черников Б. В. Архитектура информационных систем : учебное пособие. — М. : ИНФРА-М, 2020. — 256 с.

12. Tanenbaum A. S., Van Steen M. Distributed Systems: Principles and Paradigms. — 2nd ed. — Upper Saddle River : Pearson, 2017. — 686 p.
13. Newman S. Building Microservices: Designing Fine-Grained Systems. — 2nd ed. — Sebastopol : O’Reilly Media, 2021. — 600 p.
14. Zuboff S. The Age of Surveillance Capitalism. — New York : PublicAffairs, 2019. — 704 p.
15. Mozilla Foundation. Web Application Security Guide. — Mozilla Developer Network, 2023. — URL: developer.mozilla.org (дата обращения: 2025-01-03).
16. Fowler M. Patterns of Enterprise Application Architecture. — Boston : Addison-Wesley, 2003. — 533 p.
17. Kuner C., Bygrave L., Docksey C. The EU General Data Protection Regulation (GDPR): A Commentary. — Oxford : Oxford University Press, 2020. — 1920 p.
18. Kleppmann M. Designing Data-Intensive Applications. — Sebastopol : O’Reilly Media, 2017. — 616 p.
19. Черняк Л. Журналы событий и логирование в распределённых системах // Открытые системы. СУБД. — 2020. — № 4. — С. 82–90.

References

1. Federal Law of the Russian Federation of July 27, 2006, No. 152-FZ
2. "On Personal Data" (as amended as of 2025) // Collected Legislation of the Russian Federation. — 2006. — No. 31 (Part 1). — p. 3451.
3. Russian Federation. Laws. On Amendments to the Code of the Russian Federation on Administrative Offenses: Federal Law of November 30, 2024, No. 420-FZ // Official Internet Portal of Legal Information.
4. Russian Federation. Government. On Approval of Requirements for the Protection of Personal Data When Processed in Personal Data Information Systems: Resolution of the Government of the Russian Federation of November 1, 2012, No. 1119
5. Federal Service for Technical and Export Control. On approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data When Processing them in Personal Data Information Systems: Order of the FSTEC of Russia dated February 18, 2013 No. 21 (as amended on May 14, 2020): registered with the Ministry of Justice of Russia on May 14, 2013 No. 28375 // ConsultantPlus.
6. Bachilo I. L. Information Technology Law: textbook for universities. — 2nd ed., revised and enlarged. — Moscow: Yurait, 2020. — p.419
7. Kucherena A. G. Information Security and Personal Data Protection. — Moscow: Norma, 2019. — 304 p.
8. Lopatin V. N. Legal Foundations for Personal Data Protection in the Digital Environment // Journal of Russian Law. — 2021. — No. 3. — pp. 58–71.
9. Kuner C. Transborder Data Flows and Data Privacy Law. — Oxford : Oxford University Press, 2017. — p.392
10. Bass L., Clements P., Kazman R. Software Architecture in Practice. — 3rd ed. — Boston : Addison-Wesley, 2012. — p.624
11. Chernikov B. V. Architecture of Information Systems: A Tutorial. — Moscow : INFRA-M, 2020. — p.256

12. Tanenbaum A. S., Van Steen M. Distributed Systems: Principles and Paradigms. — 2nd ed. — Upper Saddle River : Pearson, 2017. — p.686
13. Newman S. Building Microservices: Designing Fine-Grained Systems. — 2nd ed. — Sebastopol: O'Reilly Media, 2021. — p. 600
14. Zuboff S. The Age of Surveillance Capitalism. — New York: PublicAffairs, 2019. — p.704
15. Mozilla Foundation. Web Application Security Guide. - Mozilla Developer Network, 2023. - URL: developer.mozilla.org (accessed 2025-01-03).
16. Fowler M. Patterns of Enterprise Application Architecture. - Boston: Addison-Wesley, 2003. - p.533
17. Kuner C., Bygrave L., Docksey C. The EU General Data Protection Regulation (GDPR): A Commentary. — Oxford : Oxford University Press, 2020. — p.1920
18. Kleppmann M. Designing Data-Intensive Applications. — Sebastopol : O'Reilly Media, 2017. — p.616
19. Chernyak L. Event logs and logging in distributed systems // Open Systems. DBMS. — 2020. — No. 4. — pp. 82–90.